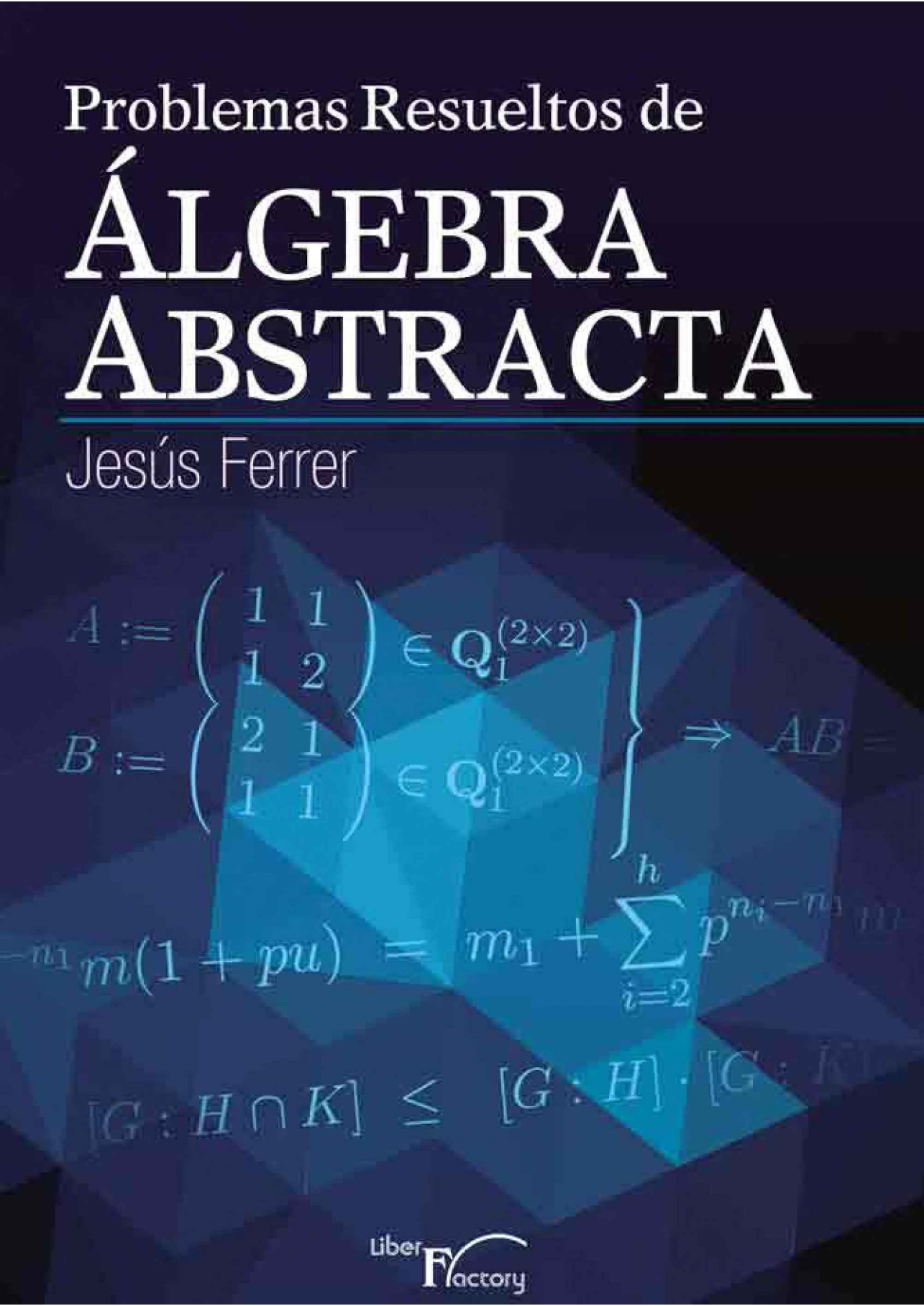
Problemas Resueltos de
ÁLGEBRA ABSTRACTA

Jesús Ferrer



Liber Factory

PROBLEMAS RESUELTOS DE ALGEBRA ABSTRACTA

Jesús Ferrer

PROBLEMAS RESUELTOS DE ALGEBRA ABSTRACTA

Jesús Ferrer

Liber Factory

Reservados todos los derechos. Queda rigurosamente prohibida, sin la autorización escrita de los titulares del *Copyright*, bajo las sanciones establecidas de las leyes, la reproducción parcial o total de esta obra por cualquier medio o procedimiento incluidos la reprografía y el tratamiento informático.

© 2014 PROBLEMAS RESUELTOS DE ALGEBRA ABSTRACTA
© Jesús Ferrer
© 2014 Editorial: Liber Factory
C/ Magnolias 35 bis 28029 Madrid. España
Web: www.liberfactory.com Tel: 0034 91 3117696

ISBN: 978-84-9949-649-8

Diseño: Andrés Sánchez

Las opiniones expresadas en este trabajo son exclusivas del autor. No reflejan necesariamente las opiniones del editor, que queda eximido de cualquier responsabilidad derivada de las mismas.

Disponible en préstamo, en formato electrónico, en
www.bibliotecavisionnet.com

Disponible en papel y ebook
www.vnetlibrerias.com
www.terrabooks.com

Pedidos a:
pedidos@visionnet.es

Si quiere recibir información periódica sobre las novedades de nuestro grupo editor envíe un correo electrónico a:
subscripcion@visionnet.es

A la memòria del meu cunyat **Eduardo**...
Força **María Teresa, Carles** i **Alex**...

Índice general

0.1. Introducción 4

1. Teoría de grupos **5**
1.1. Generalidades sobre grupos 5
1.2. Subgrupos 18
1.3. Grupos cíclicos 33
1.4. Subgrupos normales 37
1.5. Grupos actuando sobre conjuntos 51
1.6. Grupos simples 55
1.7. Homomorfismos de grupos 66
1.8. Grupos resolubles 79
1.9. El grupo simétrico 85

2. Teoría de cuerpos **99**
2.1. Generalidades y ejemplos de cuerpos 99
2.2. Polinomios sobre un cuerpo 110
2.3. Extensiones de cuerpos 124

3. Teoría de Galois **145**
3.1. El grupo de automorfismos de un cuerpo 145
3.2. Extensiones de Galois 158
3.3. Polinomios simétricos 178
3.4. Resolubilidad de ecuaciones 196

4. Teoría de anillos **207**
4.1. Generalidades y ejemplos de anillos 207
4.2. Ideales de un anillo 220
4.3. Divisibilidad en un anillo 233
4.4. Homomorfismos de anillos 241

5. Apéndice: Integrales no elementales **249**
5.1. Integrales que no salen 249
5.2. Funciones elementales 250
5.3. Teorema y Criterio de Liouville 253

0.1. Introducción

En lo que sigue presentamos la resolución de una colección de problemas de Algebra Abstracta que pretendemos sea fácilmente comprensible. La mayoría de los ejercicios están sacados del texto [2], aunque también hay algunos pocos que hemos introducido bien por ser de tipo auxiliar o bien por su atractivo. Hemos intentado que las resoluciones fuesen lo menos enfarragosas posibles cuidando en todo momento de utilizar los procedimientos más sencillos. No obstante, al tratarse de una materia que a veces se complica, puede suceder que no hayamos tenido éxito en nuestras intenciones. También conviene avisar al lector de que, al ser ésta una primera escritura de estas resoluciones, aunque la hemos revisado reiteradas veces es bastante probable que existan errores, o "gazapos", que demuestran entre otras cosas la humanidad del autor.

La primera versión, realizada manualmente en un principio, de esta colección de problemas, escrita en el curso 1987/88, fué el resultado del curso de Algebra Abstracta impartido por este autor en el Centro Asociado de la Universidad Nacional de Educación a Distancia (UNED) de Dénia (Alicante). El hecho de tener pocos alumnos presenciales y la excelente calidad e interés de éstos influyeron decisivamente en la primera intención y posterior realización de esta colección que esperamos resulte de utilidad para el público interesado.

El inicio de cada resolución se indica mediante el símbolo $\equiv$, mientras que el final lo marcamos con $\clubsuit$.

Capítulo 1

Teoría de grupos

1.1. Generalidades sobre grupos

Ex. 1 *Un semigrupo es un conjunto S dotado de un producto (operación, o ley de composición) que es estable y asociativo en S.*

a) Dado un conjunto X, demostrar que el conjunto S de todas las aplicaciones de X en sí mismo es un semigrupo para la composición de aplicaciones.

b) Demostrar que el conjunto de todas las biyecciones de X en sí mismo es un grupo para la composición.

$\equiv$

a) Representamos mediante $\circ$ la composición de aplicaciones. Claramente, si $f, g \in S$, al ser dos aplicaciones de X en X, su composición $f \circ g$ también resulta una aplicación del tipo $X \to X$, es decir, $f \circ g \in S$. Si $f, g, h \in S$, dado $x \in X$

$$((f \circ g) \circ h)(x) \;=\; (f \circ g)(h(x)) \;=\; f(g(h(x))) \;=\; f((g \circ h)(x)) \;=\; (f \circ (g \circ h))(x).$$

Lo que prueba que $(f \circ g) \circ h \;=\; f \circ (g \circ h)$.

b) Recordemos que para que una estructura monooperativa, es decir, un conjunto dotado de una operación, sea un grupo ha de cumplir cuatro propiedades: Estabilidad, asociatividad, existencia de neutro y existencia de simétrico para cada elemento (si además cumple la propiedad conmutativa, se dice que tenemos un *grupo conmutativo*, o abeliano (en honor del matemático noruego Niels Henryk Abel).

Indicamos mediante $B(X)$ al conjunto de todas las aplicaciones biyectivas de X en sí mismo. Demostramos una por una las cuatro propiedades.

Estable: Si $f, g \in B(X)$, para tener $f \circ g \in B(X)$, hay que ver que $f \circ g$ es biyectiva. Si $x, y \in X$ son tales que $(f \circ g)(x) = (f \circ g)(y)$, entonces

$$(f \circ g)(x) = (f \circ g)(y) \;\Rightarrow\; f(g(x)) = f(g(y)) \;\Rightarrow\; [f \textit{ inyectiva}]\; g(x) = g(y)$$

$$\Rightarrow\; [g \textit{ inyectiva}]\; x = y.$$

Es decir, $f \circ g$ es inyectiva. Veamos que también es sobre (o exhaustiva, o suprayectiva): Si $y \in X$,

$$[f \text{ sobre}] \Rightarrow \exists x_1 \in X / f(x_1) = y \Rightarrow [g \text{ sobre}] \exists x_2 \in X / g(x_2) = x_1 \Rightarrow (f \circ g)(x_2)$$

$$= f(g(x_2)) = f(x_1) = y.$$

Asociativa: Se cumple en general siempre que compongamos aplicaciones, como vimos en el apartado anterior.
Neutro: La aplicación $Id_X : X \to X$ tal que, $\forall x \in X$, $Id_X(x) = x$, se llama *Identidad en* X y es evidente verificar que es el elemento neutro de la estructura $(B(X), \circ)$: Primero, $Id_X \in B(X)$, ya que es una biyección de X en X. Después, si $f \in B(X)$, entonces, dado $x \in X$,

$$\left.\begin{array}{l} (f \circ Id_X)(x) = f(Id_X(x)) = f(x) \ \to \ f \circ Id_X = f \\ (Id_X \circ f)(x) = Id_X(f(x))) = f(x) \ \to \ Id_X \circ f = f \end{array}\right\} \ \Rightarrow \ f \circ Id_X = f \circ Id_X = f.$$

Simétricos: Dada $f \in B(X)$, por ser biyectiva sabemos que su *aplicación inversa, o recíproca*, f^{-1}, existe y también es biyectiva. Por tanto, $f^{-1} \in B(X)$. Además, por definición de f^{-1}, se tiene que

$$f \circ f^{-1} \ = \ f^{-1} \circ f \ = \ Id_X \ . \clubsuit$$

Nota 1 En general, siempre que el conjunto X tenga más de dos elementos, se puede comprobar sin dificultad que $(B(X), \circ)$ es un grupo no conmutativo. Suponiendo que a, b, c son tres elementos distintos de X, consideremos las siguientes biyecciones:

$$\left.\begin{array}{l} f : X \to X \text{ tal que : } \forall x \in X \setminus \{a,b,c\}, \ f(x) = x; \ f(a) = b; \ f(b) = c; \ f(c) = a \\ g : X \to X \text{ tal que : } \forall x \in X \setminus \{a,b,c\}, \ g(x) = x; \ g(a) = b; \ g(b) = a; \ g(c) = c \end{array}\right\}$$

$$\Rightarrow \left\{\begin{array}{l} (f \circ g)(a) = f(g(a)) = f(b) = c \\ (g \circ f)(a) = g(f(a)) = g(b) = a \end{array}\right\} \ \Rightarrow \ f \circ g \ \neq \ g \circ f.$$

Ex. 2 *Sea S un semigrupo (no ponemos símbolo alguno para indicar su operación, es decir, trabajamos similarmente a como representamos el producto numérico). Sea $e \in S$ tal que $ea = ae = a$, para cualquier elemento $a \in S$. Demostrar que e es único. A este elmento único e se le llama neutro, o neutro bilátero.*

$\equiv$

Sea $e' \in S$ tal que $ae' = e'a = a$, para cualquier $a \in S$. En particular, tomando $a = e$, y aplicando la propiedad de e, se tiene

$$\left.\begin{array}{l} ee' \ = \ e'e \ = \ e \\ ee' \ = \ e'e \ = \ e' \end{array}\right\} \ \Rightarrow \ e = e'. \clubsuit$$

Ex. 3 *Sea S un semigrupo. Sea $e \in S$ tal que $ea = a$ (neutro por la izquierda), para cualquier elemento $a \in S$. Si para cada $a \in S$, existe un único $a^{-1} \in S$ tal que $a^{-1}a = e$ (simétrico por la izquierda), demostrar que S es un grupo.*

≡

Al ser S semigrupo ya sabemos que su operación es estable y asociativa. Nos falta verificar que admite elemento neutro y que cada elemento tiene un simétrico. Como cabe esperar, el candidato natural a neutro es e y, para cada $a \in S$, el candidato natural a simétrico de a es a^{-1}. Observemos que, dados $a, b \in S$, $(ab)^{-1} = b^{-1}a^{-1}$, ya que:

$$(b^{-1}a^{-1})(ab) = (b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e \ [unicidad] \Rightarrow (ab)^{-1} = b^{-1}a^{-1}.$$

Ahora veamos que $e^{-1} = e$

$$e^{-1} = ee^{-1} = ((e^{-1})^{-1}e^{-1})e^{-1} = (e^{-1})^{-1}(e^{-1}e)e^{-1} = (e^{-1})^{-1}(ee^{-1}) = (e^{-1})^{-1}e^{-1} = e.$$

Por tanto

$$a^{-1} = (ea)^{-1} = a^{-1}e^{-1} = a^{-1}e.$$

Además, de lo previo

$$(a^{-1})^{-1} = (a^{-1})^{-1}e = (a^{-1})^{-1}(a^{-1}a) = ((a^{-1})^{-1}a^{-1})a = ea = a.$$

Luego

$$ae = (a^{-1})^{-1}e = (a^{-1})^{-1} = a.$$

Es decir, $ea = ae = a$. También, de lo hecho antes

$$aa^{-1} = (a^{-1})^{-1}a^{-1} = e,$$

de donde queda claro que $a^{-1}a = aa^{-1} = e$, es decir, a^{-1} es el simétrico de a. ♣

Ex. 4 *Sea S un semigrupo finito tal que: $xy = xz$, ó, $yx = zx$, implica que $y = z$. Demostrar que S es un grupo.*

≡

Sea $x \in S$. Como el conjunto $\{x^n : n \in \mathbf{N}\}$ es finito (al escribir x^n significamos el elemento que se obtiene al operar x consigo mismo n veces, o sea, $x^n = xx \overset{(n)}{\cdots} x$), existen $n, m \in \mathbf{N}$, $n > m$ tales que $x^n = x^m$. Sea $p := n - m \geq 1$. Entonces

$$x^{m-1}x = x^{m-1}x^{p+1} \rightarrow x = x^{p+1}.$$

Como en el ejercicio anterior, sólo tenemos que comprobar que S admite neutro, que llamaremos e, y que cada elemento de S admite simétrico. Primero veamos que $e = x^p$: Dado $y \in S$,

$$\left.\begin{array}{l} xy = x^{p+1}y = x(x^p y) \rightarrow y = x^p y \\ yx = yx^{p+1} = (yx^p)x \rightarrow y = yx^p \end{array}\right\} \Rightarrow x^p = e.$$

Considerando el x arbitrario anterior, como $x^p = e$, tenemos

$$\left.\begin{array}{l} e = x^p = xx^{p-1} \\ e = x^p = x^{p-1}x \end{array}\right\} \Rightarrow x^{-1} = x^{p-1}. \ ♣$$

Ex. 5 *Sea G un grupo. Definimos $x * y := yx$, para cualquier $x, y \in G$. Demostrar que $(G, *)$ es un grupo (el grupo opuesto de G).*

≡

Verifiquemos las propiedades de estructura de grupo para $(G, *)$.
Estable: Si $x, y \in G$, $x * y = yx \in G$, ya que el producto de G es estable en G.
Asociativa: Si $x, y, z \in G$, $(x * y) * z = (yx) * z = z(yx) = (zy)x = x * (zy) = x * (y * z)$.
Neutro: Si $e \in G$ es el neutro de G, veamos que también es el neutro de $(G, *)$: $\forall x \in G$,

$$\left.\begin{array}{l} e * x = xe = x \\ x * e = ex = x \end{array}\right\} \Rightarrow \quad e * x = x * e = x.$$

Simétricos: Si $x \in G$, sabemos que existe $x^{-1} \in G$ tal que $xx^{-1} = x^{-1}x = e$. Entonces

$$\left.\begin{array}{l} e = xx^{-1} = x^{-1} * x \\ e = x^{-1}x = x * x^{-1} \end{array}\right\} \Rightarrow \quad x * x^{-1} = x^{-1} * x = e. \ \clubsuit$$

Ex. 6 *Sean G y G' dos grupos. En el producto cartesiano $G \times G'$, definimos $(x, x')(y, y') := (xy, x'y')$. Demostrar que $G \times G'$ es un grupo para este nuevo producto (el producto directo de G y G').*

≡

Como siempre en estos casos, hay que verificar el cumplimiento de las cuatro propiedades definitorias de la estructura de grupo.
Estable: Si $(x, x'), (y, y') \in G \times G'$, claramente $(x, x')(y, y') := (xy, x'y')$ pertenece a $G \times G'$.
Asociativa: Si $(x, x'), (y, y'), (z, z') \in G \times G'$,

$$[(x, x')(y, y')](z, z') = (xy, x'y')(z, z') = ((xy)z, (x'y')z') = (x(yz), x'(y'z'))$$

$$= (x, x')(yz, y'z') = (x, x')[(y, y')(z, z')].$$

Neutro: Si $e \in G$ es el neutro de G y $e' \in G'$ es el neutro de G', veamos que $(e, e') \in G \times G'$ es el neutro de $G \times G'$: $\forall (x, x') \in G \times G'$,

$$\left.\begin{array}{l} (x, x')(e, e') = (xe, x'e') = (x, x') \\ (e, e')(x, x') = (ex, e'x') = (x, x') \end{array}\right\} \Rightarrow \quad (x, x')(e, e') = (e, e')(x, x') = (x, x').$$

Simétricos: Si $(x, x') \in G \times G'$, sean $x^{-1} \in G$ y $x'^{-1} \in G'$ los simétricos de x y x', respectivamente. Veamos que $(x^{-1}, x'^{-1}) \in G \times G'$ es el simétrico de (x, x') en $G \times G'$:

$$\left.\begin{array}{l} (x, x')(x^{-1}, x'^{-1}) = (xx^{-1}, x'x'^{-1}) = (e, e') \\ (x^{-1}, x'^{-1})(x, x') = (x^{-1}x, x'^{-1}x') = (e, e') \end{array}\right\}$$

$$\Rightarrow \quad (x, x')(x^{-1}, x'^{-1}) = (x^{-1}, x'^{-1})(x, x') = (e, e'). \ \clubsuit$$

Ex. 7 *Una simetría de una figura geométrica en sí misma es una aplicación biyectiva de la figura en sí misma que conserva las distancias entre puntos (también llamada* autocongruencia*).*

a) Demostrar que el conjunto de las simetrías de una figura dada es un grupo respecto de la composición de aplicaciones.

b) Demostrar que una simetría de un triángulo de vértices A, B, C está perfectamente determinada por la forma con que se transforman sus tres vértices.

c) Describir el grupo de las simetrías del triángulo.

≡

a) Llamamos F al conjunto de puntos que forman la figura. Por $\sigma(F)$ representamos al conjunto de las simetrías de F. Como, si $B(F)$ es el conjunto de las biyecciones de F en F, sabemos por definición que $\sigma(F) \subseteq B(F)$. Para ver que $(\sigma(F), \circ)$ es un grupo es suficiente con verificar que es subgrupo de $(B(F), \circ)$:

Dadas dos simetrías $f, g \in \sigma(F)$ y dos puntos $A, B \in F$, si por $d(\cdot, \cdot)$ indicamos la distancia,

$$d(f \circ g)(A), f \circ g)(B)) = d(f(g(A)), f(g(B)) = d(g(A), g(B)) = d(A, B) \;\Rightarrow\; f \circ g \in \sigma(F).$$

Además, si $f \in \sigma(F)$, al ser biyectiva, existe la biyección inversa f^{-1}. Veamos finalmente que $f^{-1} \in \sigma(F)$: Si A, B son puntos de F

$$d(f^{-1}(A), f^{-1}(B)) \;=\; d(f(f^{-1}(A)), f(f^{-1}(B))) \;=\; d(A, B)\ .$$

b) Representamos mediante ABC al triángulo de dichos vértices. Si $f \in \sigma(ABC)$, está claro que el conjunto $\{A, B, C\}$ es invariante por f, es decir, $f(\{A, B, C\}) = \{A, B, C\}$, lo que es consecuencia de preservar distancias. Además, supongamos que $g \in \sigma(ABC)$ es tal que $g(A) = f(A)$, $g(B) = f(B)$ y $g(C) = f(C)$. Para ver que $f = g$, sea $P \in ABC$, entonces

$$\left.\begin{array}{l} d(f(P), f(A)) = d(P, A) = d(g(P), g(A)) = d(g(P), f(A) \\ d(f(P), f(B)) = d(P, B) = d(g(P), g(B)) = d(g(P), f(B) \\ d(f(P), f(C)) = d(P, C) = d(g(P), g(C)) = d(g(P), f(C) \end{array}\right\} \;\Rightarrow\; f(P) = g(P),$$

al ser los dos puntos $f(P)$ y $g(P)$ equidistantes de los tres vértices.

c) Como cada elemento de $\sigma(ABC)$ está determinado por las imágenes de los vértices A, B, C, queda claro que se trata de indicar todas las aplicaciones biyectivas del conjunto $\{A, B, C\}$ en sí mismo. Mediante la notación $\begin{pmatrix} ABC \\ XYZ \end{pmatrix}$ queremos decir que se trata de la simetría que transforma A en X, B en Y y C en Z. Así

$$\sigma(ABC) \;=\; \{\begin{pmatrix} ABC \\ ABC \end{pmatrix}, \begin{pmatrix} ABC \\ ACB \end{pmatrix}, \begin{pmatrix} ABC \\ BAC \end{pmatrix}, \begin{pmatrix} ABC \\ BCA \end{pmatrix}, \begin{pmatrix} ABC \\ CAB \end{pmatrix}, \begin{pmatrix} ABC \\ CBA \end{pmatrix}\}. \clubsuit$$

Ex. 8 *Sea D_n el grupo de las simetrías de un polígono regular de n lados. Este grupo es conocido como el* Grupo Dihédrico*. Hallar el cardinal de D_n.*

≡ Primero observemos que este grupo es un caso particular del estudiado en el ejercicio anterior. También como antes, cada simetría queda determinada conociendo las imágenes de los vértices del polígono. Así, si indicamos dichos vértices por $\{1, 2, ..., n\}$, es obvio que D_n es un subgrupo del grupo formado por todas las biyecciones del conjunto de vértices anterior en sí mismo (al que se le llama *Grupo Simétrico* y se le representa usualmente por Σ_n). Pero, así como en el caso del triángulo, D_3 coincide con todo Σ_3, siempre que $n > 3$ podemos asegurar que D_n tiene menos cardinal que Σ_n; por cierto el cardinal de Σ_n es evidentemente $n!$, es decir, el número de permutaciones ordinarias de n objetos. El motivo de que el cardinal de D_n, para $n > 3$, sea menor que $n!$ es que en estos Σ_n siempre se pueden encontrar permutaciones σ tales que hay dos vértices i, j de modo que $d(\sigma(i), \sigma(j)) \neq d(i, j)$.

De la teoría de las isometrías en el plano, se sabe que todo elemento de D_n o bien es un *giro*, o bien es una *simetría axial*. Si representamos mediante G_n y A_n al conjunto de todos los giros del polígono respecto de su centro y al conjunto de todas las simetrías axiales, respectivamente, tenemos que $D_n = G_n \cup A_n$. Es inmediato que $G_n \cap A_n = \emptyset$, por lo que $card(D_n) = card(G_n) + card(A_n)$. Claramente, como el ángulo central del polígono es $\alpha_n := \frac{2\pi}{n}$, los giros posibles son

$$\rho_0,\ \rho_{\alpha_n},\ \rho_{2\alpha_n},\ \cdots,\ \rho_{(n-1)\alpha_n},$$

donde ρ_{α_n} indica el giro (rotación) de ángulo α_n. Por tanto, hay exactamente n giros distintos. Análogamente, las simetrías axiales son las siguientes, teniendo en cuenta que los ejes de simetría son las rectas que dividen al polígono en dos partes superponibles y por ello hay n de dichas rectas,

$$\sigma_1,\ \sigma_2, ..., \sigma_n.$$

Consecuentemente, $card(G_n) = n = card(A_n)$ y $card(D_n) = 2n$. ♣

Ex. 9 *Sea $V = \{e, a, b, c\}$ con el producto $\bullet$ dado por la siguiente tabla (también se suele llamar tabla de Cayley)*

$\bullet$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Demostrar que $(V, \bullet)$ es un grupo (es conocido como el grupo, o "Viergruppe", de Klein (Felix)).

≡ Hay que verificar el cumplimiento de las cuatro condiciones, o propiedades, de un grupo.

1) Estabilidad: Evidente, ya que $\forall x, y \in V$, $x \bullet y \in V$.

2) Asociativa: Basta con comprobar que

$$\begin{aligned} a \bullet (b \bullet c) &= a \bullet a = e \\ (a \bullet b) \bullet c &= c \bullet c = e. \end{aligned}$$

3) Neutro: Claramente, se trata del elemento e.
4) Simétricos:

Elemento	*Simétrico*
e	e
a	a
b	b
c	c.

Observar que también posee la propiedad conmutativa, por lo que $(V, \bullet)$ es un grupo abeliano. La importancia de este grupo, como veremos más adelante, radica en que junto con $\mathbf{Z}_4$ son los únicos grupos (abelianos además) de orden 4. ♣

Ex. 10 *Dado un conjunto cualquiera X, por 2^X representamos a la familia de las partes de X (el llamado conjunto potencia de X, ya que su cardinal, para X finito, coincide von el valor $2^{card(X)}$). Dados $A, B \in 2^X$, llamamos diferencia simétrica de A y B al conjunto*

$$A \diamond B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

Demostrar que $(2^X, \diamond)$ es un grupo abeliano.

≡
1) Estabilidad: $\forall A, B \in 2^X$, $A \diamond B \in 2^X$, ya que $A \diamond B$ es un subconjunto de X.
2) Conmutativa: $\forall A, B \in 2^X$, $A \diamond B = (A \cup B) \setminus (B \cap A) = (B \cup A) \setminus (A \cap B)$.
3) Asociativa: $\forall A, B, C \in 2^X$,

$$(A \diamond B) \diamond C = ((A \diamond B) \setminus C) \cup (C \setminus (A \diamond B)) = \{[(A \setminus B) \cup (B \setminus A)] \setminus C\} \cup \{C \setminus [(A \setminus B) \cup (B \setminus A)]\}$$

$$= (A \setminus B \setminus C) \cup (B \setminus A \setminus C) \cup \{[C \setminus (A \setminus B)] \cap [C \setminus (B \setminus A)]\}$$

$$= (A \setminus B \setminus C) \cup (B \setminus A \setminus C) \cup (C \setminus A \setminus B) \cup (A \cap B \cap C).$$

Análogamente, usando la conmutatividad

$$A \diamond (B \diamond C) = (B \diamond C) \diamond A = (B \setminus C \setminus A) \cup (C \setminus B \setminus A) \cup (A \setminus B \setminus C) \cup (B \cap C \cap A).$$

Consecuentemente, se tiene la igualdad deseada $(A \diamond B) \diamond C = A \diamond (B \diamond C)$.
4) Neutro: El conjunto vacío $\emptyset \in 2^X$, y cumple que, $\forall A \in 2^X$,

$$\emptyset \diamond A = (\emptyset \cup A) \setminus (\emptyset \cap A) = A \setminus \emptyset = A$$
$$A \diamond \emptyset = (A \cup \emptyset) \setminus (A \cap \emptyset) = A \setminus \emptyset = A.$$

Luego $\emptyset$ es el elemento neutro de $(2^X, \diamond)$.
4) Simétricos: $\forall A \in 2^X$, el simétrico de A es él mismo, puesto que

$$A \diamond A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset. \clubsuit$$

Ex. 11 *Definir en el intervalo abierto $]a, b[$, $a < b$, una operación de modo que resulte un grupo tal que, para cada $x \in]a, b[$, su simétrico sea $a + b - x$.*

$\equiv$ Antes de resolver el ejercicio, nos fijamos en un procedimiento bastante frecuente para transportar estructuras algebraicas de un conjunto a otro.

Lema 1 *Sean $(G,\cdot)$ un grupo y S un conjunto cualquiera tal que existe una biyección $f: G \to S$. Definiendo: $\forall x, y \in S$, $x * y := f(f^{-1}(x) \cdot f^{-1}(y))$, se obtiene un grupo $(S,*)$ que es isomorfo a $(G,\cdot)$ mediante f.*

Demostración. Verifiquemos el cumplimiento de las cuatro propiedades de grupo para $(S,*)$. Notar que decir que $x * y = f(f^{-1}(x) \cdot f^{-1}(y))$ es equivalente a que $f^{-1}(x * y) = f^{-1}(x) \cdot f^{-1}(y)$.
1) Estabilidad: $\forall x, y \in S$,

$$f^{-1}(x) \cdot f^{-1}(y) \in G \;\Rightarrow\; \exists z \in S \;/\; z = f(f^{-1}(x) \cdot f^{-1}(y)) \;\Rightarrow\; x * y = z \in S.$$

2) Asociativa: $\forall x, y, z \in S$,

$$(x * y) * z \;=\; f(f^{-1}(x * y) \cdot f^{-1}(z)) \;=\; f[f^{-1}[f(f^{-1}(x) \cdot f^{-1}(y))] \cdot f^{-1}(z)]$$

$$= f[(f^{-1}(x) \cdot f^{-1}(y))) \cdot f^{-1}(z)] \;=\; [\textit{aplicando la asociatividad de } (G,\cdot)]$$

$$= f[f^{-1}(x) \cdot (f^{-1}(y) \cdot f^{-1}(z)))] \;=\; f[f^{-1}(x) \cdot f^{-1}(y * z)] \;=\; x * (y * z).$$

3) Neutro: Si $e \in G$ es el elemento neutro del grupo $G,\cdot)$, veamos que $f(e)$ es el neutro de $(S,*)$: $\forall x \in S$,

$$\begin{aligned} x * f(e) &= f[f^{-1}(x) \cdot f^{-1}(f(e))] = f(f^{-1}(x) \cdot e) = f(f^{-1}(x)) = x \\ f(e) * x &= f[f^{-1}(f(e)) * f^{-1}(x)] = f(e \cdot f^{-1}(x)) = f(f^{-1}(x)) = x \end{aligned}$$

4) Simétricos: Dado $x \in S$, como $f^{-1}(x) \in G$ y G es un grupo, llamemos $a := f^{-1}(x)$ y sea a^{-1} el simétrico de a en G. Entonces, veamos que $f(a^{-1})$ es el simétrico de x

$$\begin{aligned} x * f(a^{-1}) &= f[f^{-1}(x) \cdot f^{-1}(f(a^{-1}))] = f(f^{-1}(x) \cdot a^{-1}) = f(a \cdot a^{-1}) = f(e) \\ f(a^{-1}) * x &= f[f^{-1}(f(a^{-1})) * f^{-1}(x)] = f(a^{-1} \cdot f^{-1}(x)) = f(a^{-1} \cdot a) = f(e), \end{aligned}$$

como $f(e)$ es el neutro de $(S,*)$ hemos concluido esta demostración.

Nos queda por ver finalmente que f es un isomorfismo de grupos. Para ello, ya que ya sabemos que es una aplicación biyectiva, todo consiste en ver que: $\forall a, b \in G$, $f(a \cdot b) = f(a) * f(b)$, lo cual es evidente de la definición de la operación $*$, si llamamos $x := f(a), y := f(b)$, entonces

$$f(a \cdot b) \;=\; f(f^{-1}(x) \cdot f^{-1}(y)) \;=\; x * y \;=\; f(a) * f(b).$$

Lema 2 *Si $I :=]-1,1[$, entonces definiendo, $\forall x, y \in I$, $x \bullet y := \frac{x+y}{1+xy}$, se obtiene que $(I,\bullet)$ es un grupo abeliano.*

Demostración.

1) Estabilidad: $\forall x, y \in I$, de las desigualdades $\begin{cases} (1-x)(1-y) > 0 \\ (1+x)(1+y) > 0 \end{cases}$ obtenemos $-1 - xy < x + y < 1 + xy$, es decir, $\mid x + y \mid < 1 + xy$, de donde

$$\mid x \bullet y \mid = \mid \frac{x+y}{1+xy} \mid < 1 \quad \Rightarrow \quad x \bullet y \in I.$$

2) Asociativa: $\forall x, y, z \in I$,

$$\begin{aligned} (x \bullet y) \bullet z &= (\tfrac{x+y}{1+xy}) \bullet z = \tfrac{(\frac{x+y}{1+xy})+z}{1+(\frac{x+y}{1+xy})z} = \tfrac{x+y+z+xyz}{1+xy+xz+yz} \\ x \bullet (y \bullet z) &= x \bullet (\tfrac{y+z}{1+yz}) = \tfrac{x+(\frac{y+z}{1+yz})}{1+x(\frac{y+z}{1+yz})} = \tfrac{x+y+z+xyz}{1+xy+xz+yz} \end{aligned}$$

3) Neutro: El neutro es el 0, veámoslo: $\forall x \in I$,

$$\begin{aligned} x \bullet 0 &= \tfrac{x+0}{1+x\cdot 0} = x \\ 0 \bullet x &= \tfrac{0+x}{1+0\cdot x} = x. \end{aligned}$$

Observar que $0 \in I$.

4) Simétricos: Dado $x \in I$, veamos que $-x \in I$ es el simétrico de x

$$\begin{aligned} x \bullet (-x) &= \tfrac{x+(-x)}{1+x\cdot(-x)} = 0 \\ (-x) \bullet x &= \tfrac{(-x)+x}{1+(-x)\cdot x} = 0. \end{aligned}$$

5) Conmutativa: $\forall x, y \in I$,

$$x \bullet y = \frac{x+y}{1+xy} = \frac{y+x}{1+yx} = y \bullet x.$$

Volviendo a nuestro ejercicio, notemos primero que la función $f : I \to]a, b[$ tal que $f(x) := \frac{(b-a)x+a+b}{2}$ es una biyección (se trata de la recta que une los puntos $(-1, a)$ y $(1, b)$). Por tanto, aplicando el Lemma 1, podemos transportar la estructura del grupo $(I, \bullet)$ al intervalo $]a, b[$ definiendo ahí una operación de la forma: $\forall x, y \in]a, b[$, $x * y := f(f^{-1}(x) \bullet f^{-1}(y))$. Del Lema 2, sabemos que el grupo $(I, \bullet)$ es abeliano, por lo que podemos afirmar que el nuevo grupo obtenido $(]a, b[, *)$ también lo es. Vamos a explicitr un poco mejor como actúa el nuevo grupo. Si $x, y \in]a, b[$, haciendo operaciones (cuentas, que se llaman...)

Llamando: $s := f^{-1}(x), t := f^{-1}(y)$, tenemos: $s = \frac{2x-a-b}{b-a}$, $t = \frac{2y-a-b}{b-a}$

$$\begin{aligned} x * y &= f(f^{-1}(x) \bullet f^{-1}(y)) = f(s \bullet t) = f(\frac{2(x+y)-2(a+b)}{b-a}) \\ &= \frac{2(x+y)-2(a+b)+a+b}{2} = x + y - \frac{a+b}{2}. \end{aligned}$$

Así, el neutro del nuevo grupo es: $f(0) = \frac{a+b}{2}$. Por tanto, dado $x \in]a, b[$, veamos que el simétrico de x en el nuevo grupo es $a + b - x$, como pide el ejercicio

$$x * (a + b - x) = x + (a + b - x) - \frac{a+b}{2} = \frac{a+b}{2}. \clubsuit$$

Nota 2 Recordando la función

$$\tanh x = \frac{\sinh x}{\cosh x} = \frac{e^x - e^{-x}}{e^x + e^{-x}}$$

puede demostrarse que se trata de un isomorfismo entre los grupos $(\mathbf{R}, +)$ y $(]-1, 1[, \bullet)$, siendo $\bullet$ la operación antes definida.

Ex. 12 *Sea G un grupo. Dado $a \in G$, demostrar que la aplicación $f_a : G \to G$ tal que $f_a(x) = ax$ es inyectiva.*

$\equiv$ Como se observa, no usamos símbolo alguno para la operación de G, éso lo hace todo más cómodo.

Para ver que la aplicación f_a es inyectiva, tomemos dos elementos $x, y \in G$ tales que $f_a(x) = f_a(y)$. Entonces, si como cabe esperar a^{-1} es el inverso de a,

$$f_a(x) = f_a(y) \;\Rightarrow\; ax = ay \;\Rightarrow\; a^{-1}(ax) = a^{-1}(ay) \;\Rightarrow\; (a^{-1}a)x = (a^{-1}a)y \;\Rightarrow\; x = y. \clubsuit$$

Nota 3 A la propiedad del ejercicio anterior, que nos dice que en un grupo, si $xy = xz$, entonces $y = z$, se le llama propiedad *cancelativa, o simplificativa.*

Ex. 13 *Si $f : G \to G'$ es un homomorfismo de grupos, es decir, una aplicación tal que, $\forall x, y \in G$, $f(xy) = f(x)f(y)$, demostrar que f conserva los neutros y los inversos.*

$\equiv$ Llamando e y e' a los neutros de G y de G', respectivamente, veamos que $f(e) = e'$: Si $x \in G$

$$f(x)e' = f(x) = f(xe) = f(x)f(e) \;\Rightarrow\; [\textit{aplicando la propiedad cancelativa}] \;\Rightarrow\; e' = f(e).$$

Si $x \in G$, entonces

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e' = f(x)f(x)^{-1}$$

$$\Rightarrow\; [\textit{aplicando la propiedad cancelativa}] \;\Rightarrow\; f(x^{-1}) = f(x)^{-1}. \clubsuit$$

Ex. 14 *Supongamos que en un conjunto S se tiene una aplicación (o ley de composición interna) $| : S \times S \to S$ que cumple dos propiedades:*

(i) Existe un elemento $l \in S$ tal que: $a|b = l \leftrightarrow a = b$.

(ii) $\forall a, b, c \in S$, $(a|c)|(b|c) = a|b$.

Demostrar que, definiendo en S $a \cdot b := a|(l|b)$, se obtiene una estructura de grupo para $(S, \cdot)$.

$\equiv$ Primero demostramos los siguientes resultados de apoyo: $\forall x, y \in S$

(1) $l|(x|y) = y|x$: Ya que $l|(x|y) = (y|y)|(x|y) = y|x$.

(2) $(x|y)|l = x|y$: Ya que $(x|y)|l = (x|y)|(y|y) = x|y$.

(3) $x|l = x$: Ya que $(x|l)|x = ((x|l)|l)|(x|l) = (x|l)|(x|l) = l \;\Rightarrow\; x|l = x$.

(4) $(x|(l|y))|y = x$: Ya que $(x|(l|y))|y = (x|(l|y))|(y|l) = (x|(l|y))|(l|(l|y)) = x|l = x$.

Verificamos seguidamente las propiedades de grupo para $(S, \cdot)$.
Estabilidad: $\forall x, y \in S$, $x \cdot y = x|(l|y) \in S$, ya que $|$ es estable en S.
Asociatividad: $\forall x, y, z \in S$,

$$\begin{array}{l}(x \cdot y) \cdot z = (x \cdot y)|(l|z) = (x|(l|y))|(l|z) = ((x|(l|y))|y)|((l|z)|y) \\ = [de\ (4)] = x|((l|z)|y) \\ x \cdot (y \cdot z) = x|(l|(y \cdot z)) = x|(l|(y|(l|z))) = [de\ (1)] = x|((l|z)|y).\end{array}$$

Neutro: $\forall x \in S$,

$$\begin{array}{l}x \cdot l = x|(l|l) = x|l = [de\ (3)] = x \\ l \cdot x = l|(l|x) = [de\ (1)] = x|l = x.\end{array}$$

Luego el neutro de $(S, \cdot)$ es l.
Simétricos: $\forall x \in S$, veamos que el simétrico de x en $(S, \cdot)$ es $l|x$:

$$\begin{array}{l}x \cdot (l|x) = x|(l|(l|x)) = [de\ (1)] = x|(x|l) = [de\ (3)] = x|x = l \\ (l|x) \cdot x = (l|x)|(l|x) = l. \clubsuit\end{array}$$

Ex. 15 *Indicar cuales de las siguientes estructuras son grupos abelianos:*

1) $(\mathbf{Q}, +)$; $(\mathbf{Q}, \cdot)$.

2) $(\mathbf{Q} \setminus \{0\}, +)$; $(\mathbf{Q} \setminus \{0\}, \cdot)$.

3) $(\mathbf{Q}^+, +)$; $(\mathbf{Q}^+, \cdot)$, *siendo* $\mathbf{Q}^+$ *el subconjunto de* $\mathbf{Q}$ *formado ppor todos los racionales positivos.*

4) $(\mathbf{Q}^{(2\times 2)}, +)$; $(\mathbf{Q}^{(2\times 2)}, \cdot)$, *donde* $\mathbf{Q}^{(2\times 2)}$ *representa al conjunto de las matrices cuadradas* (2×2) *de coeficientes racionales.*

5) $(\mathbf{Q}_1^{(2\times 2)}, +)$; $(\mathbf{Q}_1^{(2\times 2)}, \cdot)$, *donde* $\mathbf{Q}_1^{(2\times 2)}$ *representa al subconjunto de* $\mathbf{Q}^{(2\times 2)}$ *formado por todos los elementos de determinante igual a* 1.

$\equiv$

1) $(\mathbf{Q}, +)$ es grupo abeliano. $(\mathbf{Q}, \cdot)$ no es grupo, ya que $0 \in \mathbf{Q}$ no admite inverso.

2) $(\mathbf{Q} \setminus \{0\}, +)$ no es grupo, pues no tiene elemento neutro. $(\mathbf{Q} \setminus \{0\}, \cdot)$ es grupo abeliano.

3) $(\mathbf{Q}^+, +)$ no es grupo, ya que, como $\mathbf{Q} = \{x \in \mathbf{Q} : x > 0\}$, ni tiene neutro ni simétricos. $(\mathbf{Q}^+, \cdot)$ es grupo abeliano, gracias a la regla de los signos.

4) $(\mathbf{Q}^{(2\times 2)}, +)$ es grupo abeliano. $(\mathbf{Q}^{(2\times 2)}, \cdot)$ no es grupo, puesto que las matrices singulares (determinante nulo) no tienen inverso.

5) $(\mathbf{Q}_1^{(2\times 2)}, +)$ no es grupo, ya que, si $A \in \mathbf{Q}_1^{(2\times 2)}$ se tiene que $det(A) = 1$; pero $de(-A) = (-1)^2 det(A) = 1$ implica que $-A \in \mathbf{Q}_1^{(2\times 2)}$; sin embargo $A + (-A) = \mathbf{0}$ (matriz nula) claramente no pertenece a $\mathbf{Q}_1^{(2\times 2)}$.

Veamos que $(\mathbf{Q}_1^{(2\times 2)}, \cdot)$ es grupo pero no abeliano.
Estable: $\forall A, B \in \mathbf{Q}_1^{(2\times 2)}$, $det(AB) = det(A)det(B) = 1 \cdot 1 = 1$, luego $AB \in \mathbf{Q}_1^{(2\times 2)}$.
Asociativa: Es bien sabido que el producto de cualesquiera matrices multiplicables siempre es asociativo.
Neutro: Si por I_2 indicamos la matriz unidad de orden 2, resulta evidente que I_2 es la matriz neutra para el producto y además $det(I_2) = 1$, luego $I_2 \in \mathbf{Q}_1^{(2\times 2)}$.

Simétricos: Si $A \in \mathbf{Q}_1^{(2\times 2)}$, como $det(A) = 1 \neq 0$, A admite matriz inversa A^{-1} y claramente $A^{-1} \in \mathbf{Q}_1^{(2\times 2)}$, ya que $det(A^{-1} = \frac{1}{det(A)} = 1$. A todo ésto, no hemos mencionado que estamos aprovechándonos todo el rato de que los coeficientes de las matrices son elementos de $\mathbf{Q}$ que, al ser un *cuerpo conmutativo*, es estable para las sumas y productos.
No abeliano: Basta con tomar un contraejemplo adecuado. Sean

$$\left.\begin{array}{l} A := \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \in \mathbf{Q}_1^{(2\times 2)} \\ B := \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in \mathbf{Q}_1^{(2\times 2)} \end{array}\right\} \Rightarrow AB = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \neq BA = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}. \clubsuit$$

Ex. 16

a) Demostrar que todo grupo de cardinal menor o igual que 5 *es abeliano.*
b) Definir un grupo de 6 *elementos no abeliano.*
c) Construir un grupo de 6 *elementos que sea abeliano.*

≡

a) Sea G un grupo de cardinal menor o igual a 5. Supongamos que existen dos elementos $a, b \in G$ tales que $ab \neq ba$. Si e es el neutro de G, podemos afirmar que

$$a \neq b,\ \ a \neq e,\ b \neq e,\ ab \neq a,\ ab \neq b,\ ba \neq a,\ ba \neq b,\ ab \neq e,\ ba \neq e.$$

Para comprenderlo, si $ab = a$, entonces $ab = ae \rightarrow$ [cancelando] $b = e$, que no puede ser. Si $ab = e$, entonces $b = a^{-1}$ y $ab = aa^{-1} = e = a^{-1}a = ba$, que no es así.

Por tanto, e, a, b, ab, ba son elementos distintos de G, con lo que $G = \{e, a, b, ab, ba\}$. Veamos que ello nos conduce a un absurdo: Para ello basta con verificar que ningún elemento del tal G puede ser a^{-1}:

$$\begin{array}{l} Si\ a^{-1} = e \ \rightarrow\ e = aa^{-1} = ae = a,\ absurdo \\ Si\ a^{-1} = a \ \rightarrow\ aa = e \ \rightarrow \left\{\begin{array}{l} Si\ aba = e \rightarrow ba = a, absurdo \\ Si\ aba = a \rightarrow ba = e, absurdo \\ Si\ aba = b \rightarrow ba = ab, absurdo \\ Si\ aba = ab \rightarrow ba = b, absurdo \\ Si\ aba = ba \rightarrow ab = b, absurdo \end{array}\right. \\ Si\ a^{-1} = b \ \rightarrow\ c = ab,\ absurdo \\ Si\ a^{-1} = ab \ \rightarrow\ e = aab,\ e = aba \rightarrow\ aab = aba \rightarrow\ ab = ba,\ absurdo \\ Si\ a^{-1} = ba \ \rightarrow\ e = aba,\ e = baa \rightarrow\ ab = ba,\ absurdo. \end{array}$$

Así, como la conclusión obtenida finalmente es un absurdo, podemos afirmar que nuestra suposición de partida es falsa, es decir, G es un grupo abeliano.
b) Consideremos el *grupo simétrico* de 3 elementos, es decir,

$$\Sigma_3 = \{(123), ((132), (213), (231), (312), (321)\}.$$

Claramente este grupo no es abeliano, ya que [recordar que al escribir (xyz) indicamos que la imagen de 1 por esta permutación es x, la de 2 es y y la de 3 es z],

$$(132)(213) = (312);\ \ (213)(132) = (231),$$

luego $(132)(213) \neq (213)(132)$, es decir, Σ_3 no es abeliano. Por si acaso, si llamamos $f = (132)$ y $g = (213)$, los cálculos realizados se justifican así

$$\left\{\begin{array}{l}(fg)(1) = f(g(1)) = f(2) = 3\\(fg)(2) = f(g(2)) = f(1) = 1\\(fg)(3) = f(g(3)) = f(3) = 2\end{array}\right\}$$
$$\left\{\begin{array}{l}(gf)(1) = g(f(1)) = g(1) = 2\\(gf)(2) = g(f(2)) = g(3) = 3\\(gf)(3) = g(f(3)) = g(2) = 1.\end{array}\right\}$$

c) Un ejemplo de grupo abeliano de 6 elementos es el de las *clases residuales módulo* 6

$$\mathbf{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$$

provisto de la suma; es decir, si $\overline{x}, \overline{y} \in \mathbf{Z}_6$, entonces $\overline{x} + \overline{y} = \overline{x+y}$, donde la clase residual $\overline{x+y}$ se considera reducida en módulo 6. Por ejemplo

$$\overline{3} \ + \ \overline{5} \ = \ \overline{8} \ = \ \overline{2},$$

ya que el resto de la divisón de 8 entre 6 es 2. ♣

Ex. 17 *Demostrar que, para $n > 2$, el grupo dihédrico D_n no es abeliano.*

≡

De un ejercicio anterior, sabemos que $D_n = G_n \cup A_n$, donde G_n es el subgrupo de los giros (permutaciones cíclicas crecientes) y A_n es el subconjunto de las simetrías axiales (permutaciones cíclicas decrecientes). Es más, si llamamos:

$$\rho \ := \ (2, 3, ..., n, 1); \quad \sigma \ := \ (n, n-1, ..., 2, 1),$$

se tiene que

$$\left.\begin{array}{l}G_n = \{\rho^0, \rho^1, \rho^2, ..., \rho^{n-1}\}\\A_n = \{\sigma, \rho\sigma, \rho^2\sigma, ..., \rho^{n-1}\sigma\}\end{array}\right\} \ \Rightarrow \ G_n = \{\rho^0, \rho^1, \rho^2, ..., \rho^{n-1}\} \cup \{\sigma, \rho\sigma, \rho^2\sigma, ..., \rho^{n-1}\sigma\}.$$

Entonces

$$\left.\begin{array}{l}\rho\sigma(1) = \rho(n) = 1\\\sigma\rho(1) = \sigma(2) = n-1\end{array}\right\} \ \Rightarrow \ [como\ n > 2] \quad \rho\sigma \neq \sigma\rho. \ ♣$$

Ex. 18 *Sea G un grupo, de neutro e, tal que, $\forall x \in G$, $x^2 = e$. Demostrar que G es abeliano.*

≡

Dados $x, y \in G$

$$\left.\begin{array}{l}(xy)(xy) = e\\(xy)(yx) = x(yy)x = xx = e\end{array}\right\} \ \Rightarrow \ (xy)(xy) = (xy)(yx) \ [cancelando] \ \Rightarrow \ xy = yx. \ ♣$$

Ex. 19 *Demostrar que el cardinal del grupo simétrico Σ_n es $n!$.*

$\equiv$

Una forma de demostrar lo pedido consiste en observar que, como Σ_n es el conjunto de todas las biyecciones de un conjunto de n elementos en sí mismo, se trata del número de permutaciones ordinarias de n objetos que se sabe por Combinatoria que vale $n!$.

Otra forma de demostrar lo pedido consiste en realizar la demostración de la afirmación anterior usando el método de inducción. Es decir, dado un conjuto $S_n = \{1, 2, 3, ..., n\}$ queremos ver que el cardinal del conjunto Σ_n de todas las biyecciones de S_n en sí mismo es $n!$.

Para $n = 1$. $S_1 = \{1\}$ y sólo hay una aplicación (la identidad)m de S_1 en S_1; es decir, $card(\Sigma_1) = 1 = 1!$.

Suponiendo que la afirmación vale para n, veámosla para $n+1$: Para ello, consideramos la aplicación $T : \Sigma_n \times S_{n+1} \to \Sigma_{n+1}$ definida del siguiente modo, si $\sigma \in \Sigma_n$, $i \in S_{n+1}$,

$$T(\sigma, i) : \ S_{n+1} \longrightarrow \ S_{n+1} \ \ tal\ que \ \ T(\sigma, i)(j) \ = \ \begin{cases} \sigma(j), & si\ j \neq i, j \neq n+1, \\ n+1, & si\ j = i, \\ \sigma(i), & si\ j = n+1. \end{cases}$$

Se puede verificar sin mucha dificultad que T está bien definida, i.e., $T(\sigma, i) \in \Sigma_{n+1}$, así como que T es biyectiva. Por tanto

$card(\Sigma_{n+1}) \ = \ card(\Sigma_n \times S_{n+1}) \ = \ [Hipòtesis\ Inductiva] \ = \ n! \cdot (n+1) \ = \ (n+1)!$. ♣

Ex. 20 *Demostrar que, para $n > 2$, el grupo simétrico Σ_n no es abeliano.*

$\equiv$

De un ejercicio anterior, sabemos que, si $n > 2$, el grupo dihédrico D_n no es abeliano. Como D_n es un subgrupo del grupo simétrico Σ_n, resulta evidente que Σ_n no es abeliano. ♣

1.2. Subgrupos

Ex. 21 *Sea H un subconjunto no vacío de un grupo G. Demostrar que H es subgrupo de G si y sólo si se cumple que, $\forall x, y \in H, \ xy^{-1} \in H$.*

$\equiv$ Recordemos que por subgrupo entendemos un subconjunto no vacío que, al restringir a él la operación del grupo, cumple las cuatro propiedades de la estructura de grupo.
[$\Rightarrow$] Si $x, y \in H$, como H es grupo, el simétrico de y, y^{-1} pertenece a H. Por lo tanto, $xy^{-1} \in H$, ya que la operación es estable en H.
[$\Leftarrow$] Como $H \neq \emptyset$, $\exists a \in H$, de donde $e = aa^{-1} \in H$, por la hipótesis de ahora. Luego H contiene al neutro e de G. Además, si $x \in H$, como $e \in H$, de la hipótesis, $x^{-1} = ex^{-1} \in H$; es decir, todo elemento de H tiene simétrico en H. Finalmente, ya que la operación cumple de forma evidente la propiedad asociativa al cumplirla en todo G, si $x, y \in H$, como hemos visto que $y^{-1} \in H$, de nuevo la hipótesis nos dice que $xy = x(y^{-1})^{-1} \in H$, o sea, la operación es estable en H. Luego H es un subgrupo de G. ♣

Ex. 22 *Demostrar que cualquier intersección finita de subgrupos de un mismo grupo es también un subgrupo.*

≡

Sean $H_1, H_2, ..., H_n$ subgrupos del grupo G. Llamamos $H := H_1 \cap H_2 \cap ... \cap H_n$. Para ver que H es también subgrupo de G, utilizamos la caracterización demostrada en el ejercicio anterior. Así, sean $x, y \in H$. Para cada $i = 1, 2, ..., n$, se tiene que $x, y \in H_i$, por lo que, al tratarse de subgrupos, podemos afirmar que $xy^{-1} \in H_i$. Es decir, $xy^{-1} \in H_i$, para todo $i = 1, 2, ..., n$. Claramente, $xy^{-1} \in H$, como queríamos. ♣

Ex. 23

a) Si H es un subgrupo del grupo G y $a \in G$, demostrar que el conjunto $H^a := \{x \in G : \ axa^{-1} \in H\}$ es un subgrupo de G (el conjugado de H por a).

b) Sea $N(H) := \{x \in G : \ H^x = H\}$ (el normalizador de H). Demostrar que $N(H)$ es subgrupo de G y que H es subgrupo de $N(H)$.

≡

a) Primero observemos que $H^a = a^{-1}Ha$. Para la inclusión directa: Si $x \in H^a$, $axa^{-1} \in H$, luego $\exists h \in H$ tal que $axa^{-1} = h$; entonces $x = a^{-1}ha \in a^{-1}Ha$, como queríamos. Para la inclusión recíproca: Sea $x \in a^{-1}Ha$, entonces $\exists h \in H$ tal que $x = a^{-1}ha$, de lo que $axa^{-1} = h \in H$ y $x \in H^a$.

Si $x, y \in H^a$, de lo anterior, $\exists h_1, h_2 \in H$ tales que $x = a^{-1}h_1a$, $y = a^{-1}h_2a$. Por tanto,

$$xy^{-1} = (a^{-1}h_1a)(a^{-1}h_2a)^{-1} = (a^{-1}h_1a)(a^{-1}h_2^{-1}a) = a^{-1}(h_1h_2^{-1})a \in a^{-1}Ha = H^a,$$

ya que, al ser H subgrupo, $h_1h_2^{-1} \in H$.

b) Si $x, y \in N(H)$, demostrar que $xy^{-1} \in N(H)$ equivale a ver que $H^{xy^{-1}} = H$. Veámoslo, como $x^{-1}Hx = H^x = H$, $y^{-1}Hy = H^y = H$,

$$H^{xy^{-1}} = (xy^{-1})^{-1}H(xy^{-1}) = yx^{-1}Hxy^{-1} = yH^xy^{-1} = yHy^{-1} = yH^yy^{-1}$$

$$= y(y^{-1}Hy)y^{-1} = H.$$

Para ver que H es subgrupo de $N(H)$, como ambos son subgrupos de G, todo se reduce a verificar que $H \subset N(H)$: Si $x \in H$, $H^x = x^{-1}Hx = H$, ya que x y x^{-1} están en H. Por tanto, $x \in N(H)$. ♣

Ex. 24 *Demostrar que $Z_G := \{x \in G : \ \forall y \in G, \ xy = yx\}$ (el centro de G) es un subgrupo del grupo G.*

≡

Si $x, y \in Z_G$, veamos que $xy^{-1} \in Z_G$: $\forall z \in G$,

$$(xy^{-1})z = x(y^{-1}z) = x(z^{-1}y)^{-1} = x(yz^{-1})^{-1} = x(zy^{-1}) = (xz)y^{-1} = (zx)y^{-1} = z(xy^{-1}).$$ ♣

Ex. 25

a) Sea $S \subseteq G$, demostrar que existe un subgrupo mínimo del grupo G tal que contiene a S (el subgrupo generado por S, que se representa por $\langle S \rangle$).

b) Demostrar que

$$\langle S \rangle \quad = \quad \{ \ s_1 s_2 ... s_m \ : \ \ m \in \mathbf{N}, \ \forall i \in \{1, 2, ..., m\}, s_i \ \acute{o} \ s_i^{-1} \in S \ \}.$$

$\equiv$

a) Sea $\mathcal{F}$ la familia de subgrupos de G que contienen a S, i.e., $\mathcal{F} = \{H \subseteq G \ : \ H \text{ es un subgrupo de } G \text{ y } S \subseteq G\}$. Obviamente, $\mathcal{F} \neq \emptyset$, ya que $G \in \mathcal{F}$. Sabemos que $H_S := \cap_{H \in \mathcal{F}} H$ es un subgrupo de G (lo vimos en un ejercicio anterior para una cantidad finita, pero análogamente se ve para una cantidad infinita arbitraria). Además, es también evidente que H_S contiene a S, ya que cada uno de sus intersectandos lo contiene. Nos falta ver que H_S es el subgrupo de G menor posible que contiene a S, es decir, hay que probar que, si E es un subgrupo de G tal que $S \subseteq E$, entonces $H_S \subseteq E$: De la definición de H_S, como $E \in \mathcal{F}$, se tiene que $E \supseteq H_S$.

b) Como $\langle S \rangle = H_S = \ \cap_{H \in \mathcal{F}} H$, llamando

$A := \{ \ s_1 s_2 ... s_m \ : \ \ m \in \mathbf{N}, \ \forall i \in \{1, 2, ..., m\}, s_i \ \acute{o} \ s_i^{-1} \in S \ \}$, veamos que $\langle S \rangle = A$:

Para ello, antes demostramos que A es un subgrupo de G. Si $x, y \in A$, entonces $\exists m, n \in \mathbf{N}$, de modo que, si S^{-1} es el conjunto formado por todos los simétricos de los elementos de S,

$$\left.\begin{array}{l} x = s_1 s_2 ... s_m \\ y = t_1 t_2 ... t_n \\ s_1, ..., s_m, t_1, ..., t_n \in S \cup S^{-1} \end{array}\right\} \ xy^{-1} = (s_1 s_2 .. s_m)(t_1 t_2 .. t_n)^{-1} = (s_1 s_2 .. s_m)(t_n^{-1} ... t_1^{-1}) \in A.$$

Además, $A \supseteq S$, por la misma definición del conjunto A. Así pues, para demostrar que $\langle S \rangle \ = \ A$, simplemente hace falta ver que, si H es un subgrupo de G conteniendo a S, entonces $A \subseteq H$: Si $x \in A$, sabemos que $\exists m \in \mathbf{N}$ tal que $x = s_1 s_2 ... s_m$, con $s_1, ..., s_m \in S \cup S^{-1}$. Pero, como $S \subseteq H$ y H es subgrupo, se tiene que $S \cup S^{-1} \subseteq H$, por lo que $x = s_1 s_2 ... s_m \in H$, como deseábamos. ♣

Ex. 26 *El grupo dihédrico D_6 es el grupo de las simetrías de un hexágono regular $ABCDEF$. Denotamos por ρ a la rotación (giro) de 60° en sentido contrario al de las agujas del reloj, y mediante σ indicamos la reflexión (simetría axial) en el eje horizontal AD Observando la siguiente tabla se ve que $D_6 = \{\rho^i \sigma^j : \ 0 \leq i \leq 5, \ 0 \leq j \leq 1\}$.*

e	ρ	ρ^2	ρ^3	ρ^4	ρ^5	σ	$\rho\sigma$	$\rho^2\sigma$	$\rho^3\sigma$	$\rho^4\sigma$	$\rho^5\sigma$
A	B	C	D	E	F	A	B	C	D	E	F
B	C	D	E	F	A	F	A	B	C	D	E
C	D	E	F	A	B	E	F	A	B	C	D
D	E	F	A	B	C	D	E	F	A	B	C
E	F	A	B	C	D	C	D	E	F	A	B
F	A	B	C	D	E	B	C	D	E	F	A

1) Determinar el subgrupo que deja fijo a C.

2) Indicar el subgrupo en el que A, C, E permutan, demostrando que es isomorfo a D_3.
3) Hallar el subgrupo generado por $\rho^4, \rho^3\sigma$.
4) Expresar los elementos $\sigma\rho^k$, $1 \leq k \leq 5$, en la forma $\rho^i\sigma^j$.
5) Determinar el centro de D_6.

$\equiv$
1) Mirando la tabla: Llamando H_C al subgrupo de D_6 que deja fijo el vértice C, tenemos que

$$H_C \;=\; \{x \in D_6 :\; x(C) = C\} \;=\; \{\; e,\; \rho^4\sigma \;\}.$$

El hecho de que H_C sea un subgrupo es un resultado de tipo general, es decir, Si G es un grupo de biyecciones de un conjunto S en sí mismo y s es un elemento fijo de S, entonces $H_s := \{x \in G :\; x(s) = s\}$ es siempre un subgrupo de G: Si $x, y \in H_s$, como $y(s) = s$, ello nos dice que $y^{-1}(s) = s$; así, $(xy^{-1})(s) = x(y^{-1}(s)) = x(s) = s$, i.e., $xy^{-1} \in H_s$.
2) Mirando la tabla otra vez: Llamando H_{ACE} al subgrupo de D_6 formado por todas las simetrías de D_6 que permutan los vértices A, C, E, es decir, aquellas para las que el conjunto $\{A, C, E\}$ es invariante, tenemos que $H_{ACE} = \{e, \rho^2, \rho^4, \sigma, \rho^2\sigma, \rho^4\sigma\}$. Para ver que el sugrupo H_{ACE} es isomorfo al grupo simétrico $\Sigma_3 = \{(123), (132), (213), (231), (312), (321)\}$, definimos la siguiente aplicación, que fácilmente permite verificarse que es un isomorfismo de grupos, o sea, una aplicación biyectiva que conserva las operaciones: La aplicación es $T :\; H_{ACE} \to \Sigma_3$ tal que

$$\begin{aligned} T(e) &= (123) \\ T(\rho^2) &= (231) \\ T(\rho^4) &= (312) \\ T(\sigma) &= (132) \\ T(\rho^2\sigma) &= (213) \\ T(\rho^4\sigma) &= (321). \end{aligned}$$

Hacer un dibujito puede ser sumamente esclarecedor y bonito... Como es bien sabido que el grupo simétrico Σ_3 es isomorfo al grupo dihédrico D_3, acabamos de demostrar que H_{ACE} es isomorfo a D_3.
3) El subgrupo generado por $\rho^4, \rho^3\sigma$, usando la nomenclatura anteriormente fijada, es

$$\langle \rho^4, \rho^3\sigma \rangle \;=\; \{e, \rho^2, \rho^4, \rho\sigma, \rho^3\sigma, \rho^5\sigma\}.$$

4) Para $k = 1, 2, 3, 4, 5$, puede verse, a partir de la tabla, que $(\rho^{6-k}\sigma)^2 = e$, además $(\sigma\rho^k)(\rho^{6-k}\sigma) = \sigma(\rho^k\rho^{6-k})\sigma = \sigma\sigma = e$. Por tanto, $\sigma\rho^k = \rho^{6-k}\sigma$.
5) Recordemos que el suggrupo centro de D_6, Z_{D_6}, está formado por todos los elementos de D_6 que conmutan con cualquier elemento de D_6. Veamos que $Z_{D_6} = \{e, \rho^3\}$:

La inclusión recíproca es inmediata, ya que: e al ser el elemento neutro conmuta por definición con todo elemento, i.e, $e \in Z_{D_6}$; además, para $i = 1, 2, 3, 4, 5$, $\rho^3\rho^i = \rho^{3+i} = \rho^{i+3} = \rho^i\rho^3$, y $\rho^3(\rho^i\sigma) = \rho^{i+3}\sigma = \rho^i(\rho^3\sigma) = [\textit{de lo anterior}] = \rho^i(\sigma\rho^{6-3}) = (\rho^i\sigma)\rho^3$, es decir, $\rho^3 \in Z_{D_6}$.

Para demostrar la inclusión directa, sea $x \in Z_{D_6}$. Como $x \in D_6 = \{e, \rho, \rho^2, \rho^3, \rho^4, \rho^5\} \cup \{\sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma, \rho^4\sigma, \rho^5\sigma\}$, consideramos dos casos

Uno. $x = \rho^i$, $0 \leq i \leq 5$. Entonces, $\forall j \in \{0,1,2,3,4,5\}$,

$$x(\rho^j\sigma) = (\rho^j\sigma)x \;\rightarrow\; \rho^{i+j}\sigma = \rho^j\sigma\rho^i = \rho^j\rho^{6-i}\sigma = \rho^{6+j-i}\sigma \;\rightarrow\; \rho^{i+j} = \rho^{6+j-i},$$

de lo que

$$i+j \equiv 6+j-i \;(mod.\ 6) \;\rightarrow\; \exists p \in \mathbf{Z} \;/\; i+j-(6+j-i) = 6p;\; 2i-6 = 6p;\; i = 3(p+1).$$

Ello implica que i ha de ser un múltiplo de 3 dentro del conjunto $\{0,1,2,3,4,5\}$. Claramente, $i = 0$, ó, $i = 3$. Es decir, $x = e$, ó, $x = \rho^3$.

Dos. $x = \rho^i\sigma$, $0 \leq i \leq 5$. Veamos que este caso es imposible, ya que x no conmuta con todo elemento de D_6, en particular no conmuta con ρ:

$$\left.\begin{array}{l} x\rho = (\rho^i\sigma)\rho = \rho^i\rho^5\sigma = \rho^{i+5}\sigma \\ \rho x = \rho\rho^i\sigma = \rho^{i+1}\sigma \end{array}\right\} \;\Rightarrow\; \rho^{i+5} = \rho^{i+1}.$$

Ello nos lleva a que $i+5 \equiv 1+i$ $(mod.\ 6)$, de donde $\exists p \in \mathbf{Z} \;/\; i+5-(1+i) = 4 = 6p$. Absurdo. ♣

Ex. 27 *Demostrar que si X, Y, Z son subgrupos de G, e, $Y \subseteq X$, entonces $X \cap YZ = Y(X \cap Z)$.*

≡

Antes de empezar conviene observar que, si A, B son subconjuntos del grupo G, el conjunto AB se define como todos los elementos de G que admiten ser expresados como producto de un elemento de A por otro de B.

Para ver la inclusión directa, sea $x \in X \cap YZ$, entonces $x \in X$, y $\exists y \in Y$, $\exists z \in Z$, tales que $x = yz$. Pero, $x \in X$, $y \in Y \subseteq X$, $z = y^{-1}x$ implican que $z \in X \cap Z$. Luego $x = yz \in Y(X \cap Z)$.

Recíprocamente. Si $x \in Y(X \cap Z)$, existen $y \in Y$, $z \in X \cap Z$, tales que $x = yz$. Ahora bien, $z \in X$, $y \in Y \subseteq X$, implican que $x = yz \in X$. Además, $z \in Z$, de donde $x = yz \in YZ$. Es decir, $x \in X \cap YZ$. ♣

Ex. 28 *Describir el subgrupo $n\mathbf{Z} \cap m\mathbf{Z}$ de $\mathbf{Z}$.*

≡

Claramente, al referirnos al grupo $\mathbf{Z}$ queremos indicar el grupo abeliano $(\mathbf{Z}, +)$. Además, si $n \in \mathbf{N}$, por $n\mathbf{Z}$ representamos al subconjunto de $\mathbf{Z}$ formado por todos los enteros múltiplos de n. Así pues, veamos que $n\mathbf{Z} \cap m\mathbf{Z} = p\mathbf{Z}$, siendo p el mínimo común múltiplo de n, m.

Para ver la inclusión directa, sea $x \in n\mathbf{Z} \cap m\mathbf{Z}$, entonces existen $a, b \in \mathbf{Z}$ tales que $x = na = mb$. Por tanto x es múltiplo de n y de m. Consecuentemente, de la teoría de divisibilidad de los números enteros, x es un múltiplo de p, es decir, $x \in p\mathbf{Z}$. Recíprocamente, si $x \in p\mathbf{Z}$, existe $y \in \mathbf{Z}$ tal que $x = py$. Como p es múltiplo de n y de m, existen $u, v \in \mathbf{Z}$ de modo que $p = un = vm$. Así, $x = uny = vmy$, de donde queda claro que $x \in n\mathbf{Z} \cap m\mathbf{Z}$, es decir, x es un múltiplo común de n y m.

Resumiendo, hemos obtenido el siguiente resultado (de gran importancia en la Teoría de Ideales del anillo $(\mathbf{Z}, +, \cdot)$)

$$n\mathbf{Z} \cap m\mathbf{Z} \quad = \quad mcm(n,m)\mathbf{Z} \ . \ \clubsuit$$

Ex. 29 *Describir el subgrupo de* $\mathbf{Z}$ *generado por* $\{n, m\}$.

$\equiv$

Si $d := mcd(n,m)$, es decir, d es el máximo común divisor de n, m, veamos que

$$\langle\{n,m\}\rangle \quad = \quad d\mathbf{Z} \quad = \quad mcd(n,m)\mathbf{Z} \ .$$

Como hacemos frecuentemente, atacamos primero la inclusión directa: Sea $x \in \langle\{n,m\}\rangle$. Entonces, como de un ejercicio anterior sabemos que el subgrupo generado por $\{n,m\}$ está formado por todas las expresiones de la forma $s_1 + s_2 + ... + s_p + (-t_1) + (-t_2) + ... + +(-t_q)$, donde $s_1, s_2, ..., s_p, t_1, t_2, ..., t_q \in \{n,m\}$, está claro que x tiene la forma $x = pn + qm$, donde $p, q \in \mathbf{Z}$. Sean $a, b \in \mathbf{Z}$ tales que $n = ad$, $m = bd$. Así $x = pad + qbd = (pa + qb)d$. Luego $x \in d\mathbf{Z}$.

Recíprocamente, si $x \in d\mathbf{Z}$, $\exists p \in \mathbf{Z}$ tal que $x = pd$. Por el Lema de Bezout (Divisibilidad en dominios de integridad), al ser d el máximo común divisor de n y m, existen $a, b \in \mathbf{Z}$ de modo que $d = an + bm$. Por tanto, $x = p(an + bm) = pan + pbm$, es decir, x es de la forma que tienen los elementos de $\langle\{n,m\}\rangle$, por lo que $x \in \langle\{n,m\}\rangle$. $\clubsuit$

Ex. 30 *Si* $\mathbf{Z}/n$ *es el grupo aditivo de las clases residuales módulo* n*, hallar todos los subgrupos de* $\mathbf{Z}/n$.

$\equiv$

Recordemos que

$$\mathbf{Z}/n \quad = \quad \{\ \overline{0}, \overline{1}, ..., \overline{n-1}\}.$$

Consideremos el conjunto $Div(n)$ formado por todos los enteros positivos divisores de n, i.e., $Div(n) = \{d \in \mathbf{N} : \ d|n\}$. Seguidamente demostramos que H es un sbgrupo de $\mathbf{Z}/n$ si y sólo si $\exists d \in Div(n)$ tal que $H = \overline{d}(\mathbf{Z}/n)$:

$[\Rightarrow]$ Sea H un subgrupo de $\mathbf{Z}/n$. Si $H = \{\overline{0}\}$, está claro que $H = \{\overline{0}\} = \overline{n}(\mathbf{Z}/n)$, y $n \in Div(n)$. Así pues, supongamos que $H \neq \{\overline{0}\}$. Sea $p := min\{q \in \mathbf{N} : \ \overline{q} \in H\}$. Veamos que $H = \overline{p}(\mathbf{Z}/n)$: Antes veamos que $p \in Div(n)$; realizando la división entre n y p: $\exists c, r \in \mathbf{N} \cup \{0\}$ tales que $\left\{ \begin{array}{l} n = pc + r \\ 0 \leq r < p \end{array} \right\}$, de donde $\overline{r} = \overline{n} - \overline{pc} = \overline{0} - \overline{pc} = -\overline{pc} \in H$, ello, de la definición de p, obliga a que $r = 0$, o sea, $n = pc$ y $p|n$.

Veamos la inclusión directa. Si $\overline{x} \in H$, donde $x \in \mathbf{N} \cup \{0\}$, realizando la división entre x y p: $\exists c, r \in \mathbf{N} \cup \{0\}$ tales que $\left\{ \begin{array}{l} x = pc + r \\ 0 \leq r < p \end{array} \right\}$, de donde $\overline{r} = \overline{x} - \overline{pc} \in H$. Ello implica, por definición de p, que $\overline{r} \in H$ y por tanto, de nuevo la definición de p nos dice que $r = 0$. Así $\overline{x} = \overline{pc}$, es decir, $\overline{x} \in \overline{p}(\mathbf{Z}/n)$.

Recíprocamente, Si $\overline{px} \in \overline{p}(\mathbf{Z}/n)$, existe $\overline{y} \in \mathbf{Z}/n$, $0 \leq y < n$, tal que $\overline{x} = \overline{py}$. Pero, $\overline{py} = \overline{p} + \overline{p} + \overset{(y)}{...} + \overline{p}$, luego $\overline{x} \in H$.

[$\Leftarrow$] Si $d \in Div(n)$, veamos que $\overline{d}(\mathbf{Z}/n)$ es subgrupo de $\mathbf{Z}/n$: Para ello, sean $\overline{x}, \overline{y} \in \overline{d}(\mathbf{Z}/n)$. Existen $\overline{a}, \overline{b} \in \mathbf{Z}/n$ tales que $\overline{x} = \overline{da}$, $\overline{y} = \overline{db}$. Entonces

$$\overline{x} - \overline{y} = \overline{da} - \overline{db} = \overline{d}(\overline{a} - \overline{b}) = \overline{d} \cdot \overline{a - b} \in \overline{d}(\mathbf{Z}/n). \clubsuit$$

Ex. 31 *Demostrar que el grupo aditivo* $\mathbf{Z} \times \mathbf{Z}$ *admite otros subgrupos además de los de la forma* $n\mathbf{Z} \times m\mathbf{Z}$.

$\equiv$

Consideremos $H := \langle (1,1) \rangle$, es decir, H es el subgrupo de $\mathbf{Z} \times \mathbf{Z}$ generado por el elemento $(1,1)$. Entonces $H = \{(x,x) : x \in \mathbf{Z}\}$. Veamos que H nos es del tipo $n\mathbf{Z} \times m\mathbf{Z}$: $\forall n, m \in \mathbf{Z}$, veamos que $n\mathbf{Z} \times m\mathbf{Z} \neq H$. Supongamos que $n \neq 0$, de otro modo $n\mathbf{Z} \times m\mathbf{Z} = \{(0, mx) : x \in \mathbf{Z}\}$ que claramente no coincide con H. Al ser $n \neq 0$, el conjunto $n\mathbf{Z}$ es infinito, por lo que podemos encontrar un $p \in n\mathbf{Z}$ y un $q \in m\mathbf{Z}$ tales que $p \neq q$. Obviamente, $(p,q) \in n\mathbf{Z} \times m\mathbf{Z}$, pero $(p,q) \notin H$. $\clubsuit$

Ex. 32 *Demostrar que todos los cogrupos a la izquierda de* G *respecto del subgrupo* H *tienen el mismo cardinal.*

$\equiv$

Recordemos que un cogrupo a la izquierda de G respecto del subgrupo H es un conjunto de la forma

$$xH = \{ xy : y \in H \},$$

donde x es un elemento de G. Por tanto, se trata de verificar que, si $x, y \in G$, entonces xH e yH tienen el mismo cardinal, es decir, son equipotentes. Definimos $f : xH \to yH$ tal que $f(xz) = yz$, $z \in H$. Es elemental que f está bien definida. Veamos que es biyectiva: Si $z_1, z_2 \in H$ son tales que $f(xz_1) = f(xz_2)$ ello implica que $yz_1 = yz_2$, de donde, cancelando, $z_1 = z_2$, es decir, $xz_1 = xz_2$ y f es inyectiva; para ver que también es suprayectiva, sea $u \in yH$, entonces $\exists h \in H$ tal que $u = yh$, de donde $xh \in xH$, y, $f(xh)yh = u$, como queríamos. $\clubsuit$

Ex. 33 *Sea* H *un subgrupo de* G.

a) Definir una relación binaria de equivalencia en G *que de lugar a una partición de* G *en cogrupos a la derecha respecto de* H.

b) Demostrar que el número de cogrupos a la derecha coincide con el número de cogrupos a la izquierda respecto de H.

$\equiv$

a) La relación binaria, que llamamos $\mathcal{R}$, es:

$$x\mathcal{R}y \Leftrightarrow xy^{-1} \in H.$$

Veamos que $\mathcal{R}$ es una relación de equivalencia

Reflexiva. $\forall x \in G$, $x\mathcal{R}x$, ya que $xx^{-1} = e \in H$, al ser H subgrupo.

Simétrica. Si $x\mathcal{R}y$, entonces $xy^{-1} \in H$, por tanto $(xy^{-1})^1 \in H$; pero $(xy^{-1})^1 = yx^{-1}$, luego $yx^{-1} \in H$, es decir, $y\mathcal{R}x$.

Transitiva. Si $x\mathcal{R}y$, $y\mathcal{R}z$, se tiene que $xy^{-1}, yz^{-1} \in H$, de lo que $(xy^{-1})(yz^{-1}) = xz^{-1} \in H$, ello significa que $x\mathcal{R}z$.

Para ver que define una partición en G mediante los cogrupos a la derecha respecto de H, se $x \in G$, y representemos por $\overline{x}$ a la clase de equivalencia representada por x. Entonces

$$\overline{x} = \{ y \in G : y\mathcal{R}x\} = \{ y \in G : yx^{-1} \in H\}$$
$$= \{ y \in G : \exists h \in H / yx^{-1} = h\} = \{ y \in G : \exists h \in H / y = hx\}$$
$$= \{hx : h \in H\} = Hx.$$

Es decir, las clases de equivalencia de la relación $\mathcal{R}$ son los cogrupos a la derecha respecto de H.

b) Sean $(G/H)_i$ y $(G/H)_d$ los conjuntos de los cogrupos a la izquierda respecto de H y los cogrupos a la derecha, respectivamente. Definimos $f : (G/H)_d \to (G/H)_i$ como, si $Hx \in (G/H)_d$, $f(Hx) := x^{-1}H$. Entonces, f está claramente bien definida, ya que, si $Hx = Hy$, sabemos que $x\mathcal{R}y$, de lo que $xy^{-1} \in H$, y $yx^{-1} = (xy^{-1})^{-1} \in H$, de lo que $H = yx^{-1}H$, y, $y^{-1}H = x^{-1}H$, es decir, $f(Hx) = f(Hy)$.

Veamos que f es inyectiva: Si $f(Hx) = f(Hy)$, entonces $x^{-1}H = y^{-1}H$, de donde $yx^{-1} \in H$, y, como $xy^{-1} = (yx^{-1})^{-1} \in H$, tenemos que $Hy = Hx$. Para ver que f es sobre: Sea $yH \in (G/H)_i$, entonces $Hy^{-1} \in (G/H)_d$ y además $f(Hy^{-1}) = yH$. ♣

Ex. 34 *En el grupo simétrico Σ_n definimos la relación de equivalencia: $\alpha \mathcal{R} \beta$ siempre que $\alpha(n) = \beta(n)$. Demostrar que la relación $\mathcal{R}$ es una congruencia módulo un subgrupo de Σ_n.*

≡

Consideremos el subconjunto de Σ_n dado por $H := \{ \alpha \in \Sigma_n : \alpha(n) = n\}$. Veamos que H es subgrupo de Σ_n: Si $\alpha, \beta \in H$, entonces $(\alpha\beta^{-1})(n) = \alpha(\beta^{-1}(n)) = \alpha(n) = n$, ya que $\beta(n) = n$ equivale a que $\beta^{-1}(n) = n$. Por tanto, $\alpha\beta^{-1} \in H$.

Finalmente, veamos que $\alpha \mathcal{R} \beta$ si y sólo si $\alpha^{-1}\beta \in H$:

$$\alpha \mathcal{R} \beta \Leftrightarrow \alpha(n) = \beta(n) \Leftrightarrow (\alpha^{-1}\beta)(n) = \alpha^{-1}(\beta(n)) = \alpha^{-1}(\alpha(n)) = n \Leftrightarrow \alpha^{-1}\beta \in H. \clubsuit$$

Ex. 35 *Sean H y K subgrupos de G.*

a) Demostrar que HK es subgrupo si y sólo si $HK = KH$.

b) Si HK es un subgrupo finito, demostrar que: $o(HK) = \frac{o(H)o(K)}{o(H \cap K)}$, donde $o(\cdot)$ indica el orden del subgrupo, es decir, el número de elementos que tiene.

≡

a) Supongamos que HK es subgrupo de G. Entonces, si $x \in H$, $y \in K$, como $xy \in HK$, que es subgrupo, $y^{-1}x^{-1} = (xy)^{-1} \in HK$, de lo que $\exists u \in H$, $\exists v \in K$ tales que $y^{-1}x^{-1} = uv$; ello implica que $xy = (uv)^{-1} = v^{-1}u^{-1} \in KH$, por tanto tenemos que $HK \subseteq KH$. Recíprocamente, si $x \in K$, $y \in H$, $y^{-1}x^{-1} \in HK$, así $(xy)^{-1} = y^{-1}x^{-1} \in HK$, de lo que, al ser subgrupo, $xy \in HK$, o sea, hemos demostrado que $KH \subseteq HK$. Consecuentemente, $HK = KH$.

Para ver la implicación recíproca, suponemos que $HK = KH$ y veamos que HK es subgrupo: Sean $u, v \in HK$. Entonces existen $a, b \in H$, $c, d \in K$ de modo que $u = ac$, $v = bd$. Así $uv^{-1} = (ac)(d^{-1}b^{-1}) = a(cd^{-1})b^{-1}$. Como $cd^{-1} \in K$, se tiene que $a(cd^{-1}) \in HK = KH$, por lo que existen $x \in K$, $y \in H$, tales que $a(cd^{-1}) = xy$. Entonces, $uv^{-1} = a(cd^{-1})b^{-1} = (xy)b^{-1} = x(yb^{-1}) \in KH = HK$.

b) Consideremos la aplicación $f : H \times K \to HK$ dada por $f(x, y) := xy$. Claramente, f está bien definida y llamemos $\mathcal{R}$ a la relación de equivalencia en $H \times K$ que define f, es decir,

$$(x, y)\ \mathcal{R}\ (a, b) \quad \Leftrightarrow \quad f(x, y) = f(a, b).$$

Sea ahora el conjunto $S := \{(x, x^{-1}) : x \in H \cap K\}$. Es evidente que $card(S) = o(H \cap K)$. Veamos seguidamente que toda clase de equivalencia $\overline{(a, b)}$ de $\mathcal{R}$ tiene el mismo cardinal que el conjunto S. Para ello definimos la aplicación $g : \overline{(a, b)} \to S$ tal que, $\forall (x, y) \in \overline{(a, b)}$, $g(x, y) := (x^{-1}a, by^{-1})$. Veamos que g está bien definida:

$$(x, y) \in \overline{(a, b)} \ \Rightarrow\ (x, y)\mathcal{R}(a, b) \ \Rightarrow\ f(x, y) = f(a, b) \ \Rightarrow\ xy = ab \ \Rightarrow\ yb^{-1} = x^{-1}a$$

$$\Rightarrow \begin{cases} x^{-1}a \in H \cap K \\ g(x, y) = (x^{-1}a, by^{-1}) = (x^{-1}a, (x^{-1}a)^{-1}) \in S. \end{cases}$$

g es inyectiva: Si $(x, y), (u, v) \in \overline{(a, b)}$ son tales que $g(x, y) = g(u, v)$, entonces: $\left\{ \begin{array}{l} x^{-1}a = u^{-1}a \\ by^{-1} = bv^{-1} \end{array} \right\}$, de donde, cancelando convenientemente, se obtiene que $(x, y) = (u, v)$.

Veamos ahora que g es sobre: Sea $(z, z^{-1}) \in S$, entonces $z \in H \cap K$, y tomando $\left\{ \begin{array}{l} x := az^{-1} \\ y := zb \end{array} \right\}$, tenemos que $(x, y) \in H \times K$ y

$$g(x, y) = (x^{-1}a, by^{-1}) = ((az^{-1})^{-1}a, b(zb)^{-1}) = (za^{-1}a, bb^{-1}z^{-1}) = (z, z^{-1}).$$

Como la aplicación $f : H \times K \to HK$ es sobre, sabemos que

$$o(HK) = card(HK) = card(f(H \times K)) = card(\frac{H \times K}{\mathcal{R}}).$$

Pero, de lo visto referente a que cada clase de $\frac{H \times K}{\mathcal{R}}$ tiene el mismo número de elementos que el subgrupo $H \cap K$, tenemos

$$o(H) \cdot o(K) = card(H) \cdot card(K) = card(H \times K)$$

$$= \sum_{\overline{(a,b)} \in \frac{H \times K}{\mathcal{R}}} card(\overline{(a, b)}) = card(\frac{H \times K}{\mathcal{R}}) \cdot card(H \cap K) = o(HK) \cdot o(H \cap K),$$

de donde despejando se obtiene la igualdad deseada. ♣

Ex. 36 *Determinar todos los subgrupos del grupo dihédrico D_6 y el orden de cada uno de ellos.*

$\equiv$

Mirando la tabla de Cayley de D_6, que describimos en un ejercicio anterior, si llamamos $\rho := (234561)$ (el giro de 60° en sentido contrario al reloj), $\sigma := (165432)$ (la simetría que fija los vértices $1, 4$), sabemos que, para $0 \leq i \leq 5$,

$$\begin{aligned}(\rho^i)^{-1} &= \rho^{6-i} \\ (\rho^i\sigma)^{-1} &= \rho^i\sigma.\end{aligned}$$

La siguiente table describe todos los subgrupos, con sus órdenes, de D_6:

Orden	*Subgrupos*	*Cantidad*
1	$\{e\}$	1
2	$\{e,\rho^3\},\{e,\sigma\},\{e,\rho\sigma\},\{e,\rho^2\sigma\},\{e,\rho^3\sigma\},\{e,\rho^4\sigma\},\{e,\rho^5\sigma\}$	7
3	$\{e,\rho^2,\rho^4\}$	1
4	$\{e,\rho^3,\sigma,\rho^3\sigma\},\{e,\rho^3,\rho\sigma,\rho^4\sigma\},\{e,\rho^3,\rho^2\sigma,\rho^5\sigma\}$	4
6	$\{e,\rho,\rho^2,\rho^3,\rho^4,\rho^5\},\{e,\rho^2,\rho^4,\sigma,\rho^2\sigma,\rho^4\sigma\}$	2
12	D_6	1

Para demostrar la veracidad de la tabla anterior, empecemos notando que, si H es subgrupo de D_6, entonces su orden ha de ser un divisor del orden de D_6, que como sabemos es 12. Por tanto, todo subgrupo H de D_6 ha de tener un orden $o(H)$ perteneciente al conjunto $\{1, 2, 3, 4, 6, 12\}$. Procedemos a la descripción de los subgrupos de cada uno de los órdenes posibles:

$o(H) = 1$. En todo grupo sólo hay un subgrupo unitario (de 1 elemento), se trata del conjunto que contiene al neutro, es decir, $H = \{e\}$.

$o(H) = 2$. Si $o(H) = 2$, entonces $H = \{e, x\}$, donde x es un elemento tal que $x^2 = e$. Por tanto, x ha de ser un elemento autoinverso distinto del neutro, por lo que $x \in \{\rho^3, \sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma, \rho^4\sigma, \rho^5\sigma\}$.

$o(H) = 3$. Si $o(H) = 3$, entonces $H = \{e, x, y\}$, con x, y elementos distintos tales que $xy = e$ (ya que, si por ejemplo $xy = x \to y = e$, absurdo). Así, x, y son inversos uno del otro y entonces sólo puede tratarse de $x, y \in \{\rho, \rho^2, \rho^4, \rho^5\}$. Pero, $x, y \notin \{\rho, \rho^5\}$, puesto que ρ y ρ^5 tienen orden 6 (generan un subgrupo de orden 6), lo que no puede ser ya que nuestro subgrupo H es de orden 3. Luego $x, y \in \{\rho^2, \rho^4\}$.

$o(H) = 4$. Si $o(H) = 4$, entonces $H = \{e, x, y, z\}$, siendo x, y, z elementos distintos entre sí, y de e, tales que $o(x) = o(x) = o(y) = o(z) = 2$, de lo contrario, si alguno d ellos fuese de orden mayopr quen2, tendría orden 4, lo que es imposible en D_6, repasando elm orden de cada uno de sus elementos. Así

$$x, y, z \in \{\ \rho^3,\ \sigma,\ \rho\sigma,\ \rho^2\sigma,\ \rho^3\sigma,\ \rho^4\sigma,\ \rho^5\sigma\ \}.$$

Supongamos que $y = \rho^i\sigma,\ z = \rho^j\sigma$, con $0 \leq i < j \leq 5$. Entonces

$$x = yz = (\rho^i\sigma)(\rho^j\sigma) = \rho^i(\sigma\rho^j)\sigma = \rho^i(\rho^{6-j}\sigma)\sigma = \rho^{i+6-j}\sigma^2 = \rho^{i+6-j}.$$

Como $o(x) = 2$, podemos afirmar de lo anteruior que $x = \rho^3$. Por tanto, $H = \{e, \rho^3, \rho^i\sigma, \rho^j\sigma\}$. Pero

$$\left.\begin{array}{l}0 \leq i < j \leq 5 \\ i + 6 - j = 3\end{array}\right\} \Rightarrow j = i + 3 \Rightarrow (i, j) \in \{(0, 3), (1, 4), (2, 5)\},$$

de donde se obtienen los subgrupos

$$H = \begin{cases} \{e, \rho^3, \sigma, \rho^3\sigma\}, & si\ (i,j) = (0,3), \\ \{e, \rho^3, \rho\sigma, \rho^4\sigma\}, & si\ (i,j) = (1,4), \\ \{e, \rho^3, \rho^2\sigma, \rho^5\sigma\}, & si\ (i,j) = (2,5). \end{cases}$$

$o(H) = 6$. Si $o(H) = 6$, distinguimos dos casos posibles:

Caso 1. $\rho \in H$. Entonces está claro que

$$H = \{\ e,\ \rho,\ \rho^2,\ \rho^3,\ \rho^4,\ \rho^5\ \}.$$

Caso 2. $\rho \notin H$. Ahora $\rho^5 \notin H$, por lo que H ha de contener al menos dos eklementos de la forma $\rho^i\sigma$, $\rho^j\sigma$, $0 \leq i < j \leq 5$. Si H tuviese exactamente 2 erlementos de ésa forma, se tendría que $\rho^2, \rho^3, \rho^4 \in H$; pero entonces $\rho^5 = \rho^2\rho^3 \in H$, que no puede ser. Por tanto, H contiene exactamente tres elementos $\rho^i\sigma, \rho^j\sigma, \rho^k\sigma$, con $0 \leq i < j < k \leq 5$, (observar que de tener H 4 elementos x, y, z, t de la forma indicada, los compuestos xy, xz, xt, serían potencias distintas de ρ, lo que no puede ser). Así

$$H = \{\ e, \rho^2,\ \rho^4,\ \rho^i\sigma,\ \rho^j\sigma,\ \rho^k\sigma\ \}.$$

Como

$$(\rho^i\sigma)(\rho^j\sigma) = \rho^{i+6-j} \neq \rho^{i+6-k} = (\rho^i\sigma)(\rho^k\sigma),$$

se tiene que

$$i+6-j > i+6-k \Rightarrow \left\{ \begin{array}{l} i+6-j = 4 \\ i+6-k = 2 \end{array} \right\} \Rightarrow (i,j,k) = (i, i+2, i+4) = (0,2,4).$$

Luego

$$H = \{\ e,\ \rho^2,\ \rho^4,\ \sigma,\ \rho^2\sigma,\ \rho^4\sigma\ \}.$$

Si $o(H) = 12$, es evidente que $H = D_6$. ♣

Ex. 37 *Sea G un grupo no trivial sin subgrupos propios no triviales. Demostrar que G es finito y que su orden es primo.*

≡

Los subgrupos impropios de G son $\{e\}$ y G. Por tanto, según el enunciado, si H es un subgrupo de G, H ha de ser uno de los dos impropios indicados. Como G no es trivial, $G \neq \{e\}$; así, sea $x \neq e$ tal que $x \in G$. Consideremos el subgrupo $\langle x \rangle$, entonces $\langle x \rangle \neq \{e\}$ y $\langle x \rangle$ impropio implican que $\langle x \rangle = G$. Ahora consideremos el subgrupo $\langle x^2 \rangle$. Como $\langle x^2 \rangle$ es impropio, tenemos dos posibilidades: Si $\langle x^2 \rangle = \{e\}$, se tendría $x^2 = e$ y entonces $G = \{e, x\}$, que cumple lo requerido, ya que $o(G) = 2$. Si $\langle x^2 \rangle = G$, existe un $n \in \mathbf{Z}$ tal que $x = (x^2)^n = x^{2n}$, de donde $x^{2n-1} = e$ y $o(G) = o(x) < \infty$. Veamos que $o(G)$ es un número primo: Si $o(G) = p = mn$, con $m, n \in N$, consideramos el subgrupo $\langle x^m \rangle$: si $\langle x^m \rangle = \{e\}$, entonces $x^m = e$ y, como $o(x) = o(G) = p$, $p \mid m$, de lo que $p = m$. Si $\langle x^m \rangle \neq \{e\}$, entonces $\langle x^m \rangle = G$ y $o(x^m) = p$, pero $(x^m)^n = x^p = e$, lo que implica que $p \mid n$, es decir, $p = n$. Consecuentemente, p es primo. ♣

Ex. 38 *Demostrar que todo grupo de orden par tiene un elemento de orden 2.*

≡

Sea G un grupo tal que $o(G) = 2n$. Entonces $G = \{e, x_1, x_2, ..., x_{2n-1}\}$. Dado $k \in \{1, 2, ..., 2n-1\}$, definimos $f(k) \in \{1, 2, ..., 2n-1\}$ tal que $x_{f(k)} = x_k^{-1}$. Claramente, f está bien definida, es biyectiva de $\{1, 2, ..., 2n-1\}$ en sí mismo y $x_{f(f(k))} = x_{f(k)}^{-1} = (x_k^{-1})^{-1} = x_k$ implica que $f(f(k)) = k$. El conjunto $A := \{k \in \{1, 2, ..., 2n-1\} : f(k) \neq k\}$ tiene cardinal par, ya que, $\forall k \in A$, $f(k) \in A \setminus \{k\}$; por tanto, el conjunto $\{1, 2, ..., 2n-1\} \setminus A \neq \emptyset$, con lo que, si $k \in \{1, 2, ..., 2n-1\} \setminus A$, se tiene que $f(k) = k$, es decir, $x_k^{-1} = x_{f(k)} = x_k$, o sea, $x_k^2 = e$, y $o(x_k) = 2$. ♣

Ex. 39 *Sea H el subgrupo de Σ_n formado por todas las permutaciones que dejan invariantes a n. Qué vale $[\Sigma_n : H]$?*

≡

Primero veamos que H es en efecto un subgrupo de Σ_n: Sean $\alpha, \beta \in H$, $(\alpha\beta)(n) = \alpha(\beta(n)) = \alpha(n) = n$, luego $\alpha\beta \in H$. Además, $\alpha \in H$ implica que $\alpha(n) = n$, de donde $\alpha^{-1}(n) = n$, es decir, $\alpha^{-1} \in H$.

Si consideramos la relación de equivalencia que divide a Σ_n en cogrupos a la izquierda, es decir, dados $\alpha, \beta \in \Sigma_n$, $\alpha \equiv \beta(mod.H)$ si y sólo si $\alpha^{-1}\beta \in H$, se tiene que

$$\alpha \equiv \beta(mod.H) \quad \Leftrightarrow \quad \alpha^{-1}\beta \in H \quad \Leftrightarrow \quad (\alpha^{-1}\beta)(n) = n \quad \Leftrightarrow \quad \alpha(n) = \beta(n).$$

Recordemos que $\alpha \equiv \beta(mod.H)$ si y sólo si $\alpha H = \beta H$, ya que

$$\alpha \equiv \beta(mod.H) \quad \Leftrightarrow \quad \alpha^{-1}\beta \in H \quad \Leftrightarrow \quad \beta^{-1}\alpha = (\alpha^{-1}\beta)^{-1} \in H \quad \Leftrightarrow \quad \alpha H = \beta(\beta^{-1}\alpha)H = \beta H.$$

Consideremos $\alpha_1, \alpha_2, ..., \alpha_n \in \Sigma_n$ tales que, para cada $k \in \{1, 2, ..., n\}$, $\alpha_k(n) = k$. Veamos seguidamente que el conjunto cociente $\Sigma_n/H = \{\alpha_1 H, \alpha_2 H, ...\alpha_n H\}$: Si $\beta H \in \Sigma_n/H$, sea $k := \beta(n)$, entonces $\alpha_k(n) = k = \beta(n)$, de donde, de lo visto antes, $\beta H = \alpha_k H$. La inclusión recíproca es evidente. Veamos ahora que todos los cogrupos $\alpha_k H$, $1 \leq k \leq n$, son distintos: Si $\alpha_i H = \alpha_j H$, $1 \leq i, j \leq n$, se tiene que $i = \alpha_i(n) = \alpha_j(n) = j$. Finalmente,

$$[\Sigma_n : H] \;=\; card(\Sigma_n/H) \;=\; n \;. \;\clubsuit$$

Nota 4 Otra forma de resolver el ejercicio anterior es la siguiente. Primero observemos que H es isomorfo al grupo simétrico Σ_{n-1}: Basta para verlo con considerar la aplicación $f : H \to \Sigma_{n-1}$ dada por $f(\alpha)(i) := \alpha(i)$, $i \in \{1, 2, ..., n-1\}$, $\alpha \in H$. Entonces f está bien definida, pues, como $\alpha(n) = n$, α restingida a $\{1, 2, ..., n-1\}$ es una biyección. Además, si $\alpha, \beta \in H$, $f(\alpha\beta) = f(\alpha)f(\beta)$, ya que, para $i \in \{1, 2, ..., n-1\}$,

$$f(\alpha\beta)(i) = (\alpha\beta)(i) = \alpha(\beta(i)) = \alpha(f(\beta)(i)) = f(\alpha)(f(\beta)(i)) = (f(\alpha)f(\beta))(i).$$

Para ver que f es inyectiva: Si $f(\alpha) = e' \in \Sigma_{n-1}$, $\alpha \in H$, donde e' indica el neutro de Σ_{n-1}, entonces, $\forall i \in \{1, 2, ..., n-1\}$, $\alpha(i) = f(\alpha)(i) = e'(i) = i$ y, como $\alpha(n) = n$, se deduce que $\alpha = e$, el neutro de Σ_n. Finalmente, vemos que f es sobre: Sea $\sigma \in \Sigma_{n-1}$,

definimos el elemento α de Σ_n como $\alpha(i) := \left\{ \begin{array}{l} \sigma(i), \ si \ 1 \leq i \leq n-1, \\ n, \ \ si \ \ i = n. \end{array} \right\}$ Claramente $\alpha \in H$ y $f(\alpha) = \sigma$.

Así, aplicando el Teorema de LaGrange

$$[\Sigma_n : H] \ = \ \frac{o(\Sigma_n)}{o(H)} \ = \ \frac{n!}{o(\Sigma_{n-1})} \ = \ \frac{n!}{(n-1)!} \ = \ n.$$

Ex. 40 *Sean H, K dos subgrupos de G de índice finito. Demostrar que $H \cap K$ es un subgrupo de índice finito tal que*

$$[G : H \cap K] \ \leq \ \ [G : H] \cdot [G : K].$$

$\equiv$

Para ver que $[G : H \cap K]$ es finito, supongamos que $m := [G : H]$ y $n := [G : K]$. Así, existen $x_1, x_2, ..., x_m, y_1, y_2, ..., y_n \in G$ de modo que

$$G/H \ = \ \{x_1H, x_2H, ..., x_mH\}, \quad G/K \ = \ \{y_1H, y_2H, ..., y_nH\}.$$

Para demostrar simultáneamente que $[G : H \cap K]$ es finito y que cumple la desigualdad indicada, es suficiente con verificar que

$$G/H \cap K \ \ \subset \ \ \{ \ x_iH \cap y_jH \ \ : \ \ 1 \leq i \leq m, \ 1 \leq j \leq n \ \}.$$

Para ello, si $x \in G$, como $x(H \cap K) \ = \ xH \cap xK$ (quizás la inclusión recíproca sea la menos evidente: Si $z \in xH \cap xK$, existen $u \in H$, $v \in K$ tales que $z = xu = xv$, de donde $u = v \in H \cap K$, y $z \in x(H \cap K)$), sean x_i, y_j tales que $xH = x_iH$, $xK = y_jK$, entonces $x(H \cap K) = x_iH \cap y_jK$. ♣

Ex. 41 *En un grupo G de orden finito, determinar el orden a^m, donde $a \in G$ es un elemento de orden n.*

$\equiv$

Veamos que $o(a^m) = \frac{n}{mcd(m,n)}$: Llamamos $d := mcd(m, n)$. Entonces, si $p := \frac{m}{d}$, $q := \frac{n}{d}$, se tiene que $mcd(p, q) = 1$, es decir, p, q son primos entre sí. Entonces, ya que nuestro objetivo es demostrar que $o(a^m) = q$,

$$(a^m)^q \ = \ a^{mq} \ = \ a^{\frac{mn}{d}} \ = \ a^{np} \ = \ (a^n)^p \ = \ e.$$

Finalmente, debemos ver que q es el menor número natural que cumple lo anterior, es decir, si $t \in \mathbf{N}$ es tal que $(a^m)^t = e$, veamos que $q | \ t$:

$$e \ = \ (a^m)^t \ = \ a^{mt} \ \Rightarrow \ n | \ mt \ \Rightarrow \ \exists s \in \mathbf{N} \ / \ \ mt = ns \ \Rightarrow \ pdt = qds \ \Rightarrow \ pt = qs$$

$$\Rightarrow \ q | \ pt \ \overset{mcd(p,q)=1}{\Rightarrow} \ q | \ t. \ ♣$$

Ex. 42 *Sean a, b elementos de un grupo abeliano G de orden finito. Demostrar que, si $o(a)$ y $o(b)$ son primos entre sí, entonces $o(ab) = o(a) \cdot o(b)$.*

$\equiv$

Sean $o(a) = m$, $o(b) = n$. Veamos que $o(ab) = mn$:

$$(ab)^{mn} = (ab)(ab) \overset{(mn)}{\cdots} (ab) = [\textit{al ser abeliano}] = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e \cdot e = e.$$

Además, si $q \in \mathbf{N}$ es tal que $(ab)^q = e$, entonces, como $a^q b^q = e$, se tiene que $a^q = (b^q)^{-1}$, de lo que $o(a^q) = o((b^q)^{-1}) = o(b^q)$. Aplicando el ejercicio anterior,

$$\left.\begin{array}{l} o(a^q) = o(b^q) \\ o(a^q) = \frac{m}{mcd(m,q)} \\ o(b^q) = \frac{n}{mcd(n,q)} \end{array}\right\} \Rightarrow \frac{m}{mcd(m,q)} = \frac{n}{mcd(n,q)}.$$

Entonces

$$\left.\begin{array}{l} \exists x, y \in \mathbf{Z} \ / \ mcd(m,q) = xm + yq \\ \exists x', y' \in \mathbf{Z} \ / \ mcd(n,q) = x'n + y'q \end{array}\right\} \Rightarrow m(x'n + y'q) = n(xm + yq)$$

Ahora, como $mcd(m,n) = 1$, tenemos que $m | (xm + yq)$, de lo que $m |\ yq$ y consecuentemente $m |\ mcd(m,q)$, lo que implica que $m |\ q$. De modo análogo se ve que $n |\ q$. Por tanto, al ser primos entr sí, $mn |\ q$. ♣

Ex. 43 *Demostrar que, si $a, x \in G$, entonces $o(axa^{-1}) = o(x)$.*

$\equiv$

Sea $o(x) = p$. Entonces

$$(axa^{-1})^p = (axa^{-1})(axa^{-1}) \overset{(p)}{\cdots} (axa^{-1}) = ax^p a^{-1} = aea^{-1} = e.$$

Además, si $q \in \mathbf{N}$ es tal que $(axa^{-1})^q = e$, análogamente a lo hecho antes se ve que $e = (axa^{-1})^q = ax^q a^{-1}$, de donde $ax^q = a$ y $x^q = e$. Por tanto, $p |\ q$. Luego $o(axa^{-1}) = p$. ♣

Ex. 44 *Demostrar que, en un grupo G, $o(ab) = o(ba)$, $\forall a, b \in G$.*

$\equiv$

Sea $p := o(ab)$.

$$(ba)^p = (ba)(ba) \overset{(p)}{\cdots} (ba) = b(ab)^{p-1}a \Rightarrow a(ba)^p = (ab)^p a = a \Rightarrow (ba)^p = e.$$

Además, si $q \in \mathbf{N}$ es tal que $(ba)^q = e$, procediendo como antes, $(ab)^q = e$, de donde $p |\ q$. Así $o(ba) = p$. ♣

Ex. 45 *Se G un grupo abeliano. Demostrar que, dado $n \in \mathbf{N}$, el conjunto $G_n := \{x \in G : o(x) |\ n\}$ es un subgrupo de G.*

≡

Si $x, y \in G_n$, veamos que $xy^{-1} \in G_n$: Sean $p := o(x)$, $q := o(y)$ y $m := mcm(p, q)$. Como, al tratarse de un grupo abeliano,

$$(xy^{-1})^m = x^m(y^{-1})^m = (x^p)^{\frac{m}{p}}((y^{-1})^q)^{\frac{n}{q}} = e,$$

se tiene que $o(xy^{-1})|\ m$. Ahora bien, $p|\ n$, $q|\ n$ implican que $m|\ n$ y por tanto $o(xy^{-1})|\ n$, es decir, $xy^{-1} \in G_n$. ♣

Ex. 46

a) Demostrar que sólo existen dos grupos distintos de orden 4 (salvo isomorfismos).

b) Demostrar algo similar para orden 6.

≡

a) Sea $G = \{e, x, y, z\}$. Distinguimos dos casos:

Uno. G tiene algún elemento de orden 4. Sea x alguno de ellos. Entonces $G = \{e, x, x^2, x^3\}$. Es decir, G es isomorfo al grupo aditivo $\mathbf{Z}_4$ (clases residuales módulo 4).

Dos. G no tiene elementos de orden 4. Entonces, como los órdenes han de ser divisores de 4, $o(x) = o(y) = o(z) = 2$. Razonando por exclusión se ve que: $xy = z$, $xz = y$, $yz = x$. Por tanto la tabla de G es

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e.

En este caso G es isomorfo al Viergruppe de Klein (Félix).

b) Sea $G = \{e, x, y, z, t, u\}$. Dos casos:

Uno. Si G tiene algún elemento de orden 6, está claro que G es un grupo cíclico s isomorfo al grupo aditivo $\mathbf{Z}_6$ (clases residuales módulo 6).

Dos. G no tiene elementos de orden 6. Entonces, como los órdenes han de ser divisores de 6, $o(x), o(y), o(z), o(t), o(u) \in \{2, 3\}$. Ahora consideramos dos subcasos:

(2.1) $o(x) = o(y) = o(z) = o(t) = o(u) = 2$. Veamos que ésto es imposible: Como $xy \notin \{e, x, y\}$ supongamos que $xy = z$. Entonces $xz = x^2y = y$. Pero, como $xt \notin \{e, x, y, z, t\}$, se tiene que $xt = u$ y $xu = t$. Además, $yxz = y^2 = e$ implica que $yx = z$, $yz = x$. Entonces $yt = e \rightarrow t = y$, lo que es un absurdo, ya que, por hipótesis, los elementos e, x, y, z, t, u son todos distintos.

(2.2) G tiene algún elemento de orden 3. Sea x uno de dichos elementos. Entonces $G = \{e, x, x^2, y, z, t\}$ (evidentemente todos distintos). Veamos que $o(y) = o(z) = o(t) = 2$: De no ser así, supongamos que $o(y) = 3$; ahora $G = \{e, x, x^2, y, y^2, z\}$, con lo que $o(z) = 2$, y razonando por exclusión se obtiene que $xy = yx = z$, luego $z^3 = (xy)^3 = [ya\ que\ conmutan] = x^3y^3 = 3$, lo que contradice que $z^2 = e$. Por tanto, $G = \{e, x, x^2, y, z, t\}$, con $y^2 = z^2 = t^2 = e$, de lo que se puede afirmar que G es isomorfo al grupo simétrico Σ_3, que también coincide con el grupo dihédrico D_3. ♣

Ex. 47 *Demostrar que si un grupo sólo tiene una cantidad finita de subgrupos su orden ha de ser finito.*

≡

Sea G un grupo con una cantidad finita de subgrupos. Primero veamos que todo elemento $x \in G$ es de orden finito: De lo contrario, si $o(x) = \infty$, $\forall n \in \mathbf{N}$, veamos que $\langle x^{2n} \rangle$ está estrictamente contenido en $\langle x^n \rangle$: Como la inclusión es evidente todo se reduce a verificar que $x^n \notin \langle x^{2n} \rangle$; si $x^n \in \langle x^{2n} \rangle$, existiría $p \in \mathbf{Z}$ tal que $x^n = (x^{2n})^p = x^{2pn}$, entonces $x^{(2p-1)n} = e$, lo que implica que $o(x) \leq \mid (2p-1)n \mid < \infty$, absurdo. Así, la colección

$$\langle x^n \rangle \supset \langle x^{2n} \rangle \supset \ldots$$

ofrece una cantidad infinita de subgrupos (monógenos) de G, lo que contradice la hipótesis del enunciado.

Como G tiene una cantidad finita de subgrupos, claramente sólo admite una cantidad finita de subgrupos monógenos. Sean

$$\langle x_1 \rangle, \ \langle x_2 \rangle, \ \ldots, \ \langle x_n \rangle$$

dichos subgrupos. Veamos para terminar que $G = \cup_{1 \leq i \leq n} \langle x_i \rangle$, que evidentemente es un conjunto finito al tener todos los x_i orden finito: Si $x \in G$, como $\langle x \rangle$ es un subgrupo monógeno, existe un $i \in \{1, 2, ..., n\}$ tal que $\langle x \rangle = \langle x_i \rangle$, de donde $x \in \langle x_i \rangle$. ♣

1.3. Grupos cíclicos

Ex. 48 *Determinar el número de subgrupos de orden d de un grupo cíclico de orden n.*

≡

Sea $G = \{e, x, x^2, ..., x^{n-1}\}$. Si d es el orden de algún subgrupo de G, sabemos que $d \mid n$. Vamos a ver que sólo hay un subgrupo de orden d. Para ello, si llamamos $H_0 = \langle x^{\frac{n}{d}} \rangle$, veamos que $o(H_0) = d$: Claramente, de un ejercicio anterior

$$o(H_0) \ = \ o(x^{\frac{n}{d}}) \ = \ \frac{n}{mcd(n, \frac{n}{d})} \ = \ \frac{n}{\frac{n}{d}} \ = \ d.$$

Ahora, si H es un subgrupo de G tal que $o(H) = d$, demostramos que $H = H_0$: Para ello, como H también es cíclico, existe $k \in \{1, 2, ..., n-1\}$ tal que $H = \langle x^k \rangle$. Entonces

$$d \ = \ o(H) \ = \ o(x^k) \ = \ \frac{n}{mcd(n,k)} \ \Rightarrow \ \frac{n}{d} = mcd(n,k) \ \Rightarrow \ \frac{n}{d} \mid k$$

$$\Rightarrow \ \exists p \in \mathbf{N} \ / \ k = p(\frac{n}{d}) \ \Rightarrow \ x^k = (x^{\frac{n}{d}})^p \in H_0 \ \Rightarrow \ H \subseteq H_0.$$

Como ambos subgrupos son del mismo orden, se sigue que coinciden. ♣

Ex. 49 *Sea G un grupo finito con la propiedad de que para dos subgrupos cualesquiera H, K, se tiene $H \subseteq K$, ó, $K \subseteq H$. Demostrar que G es un grupo cíclico cuyo orden es una potencia de un número primo.*

≡

Sea $G = \{x_1, x_2, ..., x_n\}$. De la hipótesis, la familia de subgrupos monógenos de G está totalmente ordenada por inclusión, así existe un $i \in \{1, 2, ..., n\}$ tal que

$$\bigcup_{j=1}^{n} \langle x_j \rangle \quad \subseteq \quad \langle x_i \rangle.$$

Claramente, $G = \langle x_i \rangle$, por lo que G es cíclico. Veamos a continuación que el orden n de G es potencia de un número primo. Suponemos que n es un número compuesto, ya que de ser primo ya habríamos terminado. Sea p un primo que es divisor de n, para ver que n es potencia de p basta con comprobar que n no admite otro factor primo. Razonando por reducción al absurdo, supongamos que existe otro primo q, distinto de p, que divide a n. Sea $x_i \in G$, tal que $\langle x_i \rangle = G$. Considerando los subgrupos $\langle x_i^{n/p} \rangle$ y $\langle x_i^{n/q} \rangle$, sabemos por hipótesis que uno está contenido en el otro, supongamos que $\langle x_i^{n/p} \rangle \subseteq \langle x_i^{n/q} \rangle$. Entonces, del Teorema de LaGrange

$$o(x_i^{n/p}) \mid o(x_i^{n/q}) \quad \Rightarrow \quad \frac{n}{mcd(n, \frac{n}{p})} \mid \frac{n}{mcd(n, \frac{n}{q})} \quad \Rightarrow \quad p \mid q,$$

lo que es contradictorio, ya que q es un número primo distinto de p. ♣

Ex. 50 *Sean G y G' dos grupos cíclicos cuyos órdenes son primos entre sí (primos relativos). Demostrar que el grupo producto $G \times G'$ también es cíclico.*

≡

Sean $G = \langle a \rangle$, $G' = \langle b \rangle$, con $o(a) = n$, $o(b) = m$, $mcd(n, m) = 1$. Todo se reduce a demostrar que $G \times G' = \langle (a, b) \rangle$: Sea $(x, y) \in G \times G'$. Existen $0 \leq i \leq n-1$, $0 \leq j \leq m-1$, tales que $x = a^i$, $y = b^j$. Como $mcd(n, m) = 1$, existen enteros r, s de modo que $1 = nr + ms$. Así $i - j = (i-j)nr + (i-j)ms$, y, llamando $k := i - (i-j)nr$, se tiene

$$j - k = j - i + (i-j)nr = (j-i)nr + (j-i)ms + (i-j)nr = (j-i)ms \Rightarrow k = j - (j-i)ms$$

$$\Rightarrow (a, b)^k = (a^k, b^k) = (a^{i-(i-j)nr}, b^{j-(j-i)ms}) = (a^i, b^j) = (x, y). \clubsuit$$

Ex. 51 *Demostrar que el producto directo de dos grupos cíclicos infinitos no es cíclico.*

≡

Sean G y G' dos grupos cíclicos infinitos. Todo consiste en demostrar que, si e, e' son el neutro de G y de G', respectivamente, dados $x \in G \setminus \{e\}$, $y \in G' \setminus \{e'\}$, entonces $\langle (x, y) \rangle \neq G \times G'$. Para ello, basta con ver que $(x, y^2) \notin \langle (x, y) \rangle$. Antes demostramos que el orden de x, y de y, es infinito. Lo vemos para x (para y es análogo): Si existiese un

$n \in \mathbf{N}$ tal que $x^n = e$, entonces, al ser G cíclico, sea $G = \langle a \rangle$; entonces existe un $m \in \mathbf{N}$ tal que $x = a^m$ y $e = x^n = a^{mn}$, lo que contradice que $o(G) = o(a)$ sea infinito.

Supongamos ahora que existe un entero n tal que $(x, y^2) = (x, y)^n = (x^n, y^n)$. Entonces

$$\left.\begin{array}{l} x = x^n \\ y^2 = y^n \end{array}\right\} \Rightarrow \left\{\begin{array}{l} x^{n-1} = e \\ y^{n-2} = e' \end{array}\right\} \Rightarrow \left\{\begin{array}{l} n-1=0 \ \rightarrow \ n=1 \\ n-2=0 \ \rightarrow \ n=2, \end{array}\right.$$

lo que es absurdo. ♣

Ex. 52 *Sea G un grupo cíclico generado por a. Averiguar qué otros elementos generan a G.*

≡

Como $G = \langle a \rangle$, podemos considerar dos casos:

Uno. G es infinito. Veamos que, en este caso, $G = \langle x \rangle$ si y sólo si $x \in \{a, a^{-1}\}$:

($\Leftarrow$) Ya sabemos que $\langle a \rangle = G$. Si $x \in G$, sabemos que existe $k \in \mathbf{Z}$ tal que $x = a^k$, entonces $x = (a^{-1})^{-k}$, es decir, $x \in \langle a^{-1} \rangle$.

($\Rightarrow$) Sea $G = \langle x \rangle$. Como $x \in G = \langle a \rangle$, existe $n \in \mathbf{Z}$ tal que $x = a^n$. Supongamos que $|n| \geq 2$, es decir que $n \notin \{1, -1\}$. Pero, como $a \in G = \langle x \rangle$, existe un $p \in \mathbf{Z}$ tal que $a = x^p$, de donde, de lo visto en el ejercicio anterior de que en un grupo cíclico infinito todo elemento distinto del neutro tiene orden infinito, tenemos

$$a = x^p = a^{np} \ \Rightarrow \ a^{np-1} = e \ \Rightarrow \ np - 1 = 0 \ \Rightarrow \ np = 1 \ \Rightarrow \ \textit{Absurdo.}$$

Luego $n \in \{1, -1\}$ y $x = a^n \in \{a, a^{-1}\}$.

Dos. G es finito. Sea $o(G) = n$. Entonces $G = \{e, a, a^2, ..., a^{n-1}\}$. Veamos que, si $k \in \{1, 2, ..., n-1\}$, entonces $G = \langle a^k \rangle$ si y sólo si $mcd(k, n) = 1$:

($\Rightarrow$) Si $G = \langle a^k \rangle$, entonces existe $p \in \mathbf{Z}$ tal que $a = (a^k)^p = a^{kp}$, de donde $a^{kp-1} = e$ y entonces $n | \ kp - 1$. Sea $q \in \mathbf{Z}$ tal que $kp - 1 = nq$, como $1 = kp + (-q)n$, del Lema de Bezout se tiene que $mcd(k, n) = 1$.

($\Leftarrow$) Supongamos que $mcd(k, n) = 1$. Aplicando otra vez el Lema de Bezout, existen $r, s \in \mathbf{Z}$ tales que $1 = rk + sn$. Entonces

$$a \ = \ a^{rk+sn} \ = \ (a^k)^r (a^n)^s \ = \ (a^k)^r \cdot e \ = \ (a^k)^r.$$

Consecuentemente

$$G \ = \ \langle \ a \ \rangle \ = \ \langle \ a^k \ \rangle.$$

Nota 5 [La función de Euler]

Se llama así a la función $\Phi : \mathbf{N} \rightarrow \mathbf{N}$ tal que, si $n \in \mathbf{N}$, entonces

$$\Phi(n) \ = \ \left\{\begin{array}{l} 1, \quad si \ n = 1, \\ \\ \textit{número de } \underline{\textit{primos con } n} \ \underline{\textit{menores que } n}, \quad si \ n \geq 2. \end{array}\right.$$

Así, una tabla de los valores primeros de Φ es la que sigue

n	$\Phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6

Es interesante conocer algunas propiedades de esta función Φ:
1) Si p es primo, entonces $\Phi(p) = p - 1$.
2) Si p es primo, entonces $\Phi(p^k) = p^{k-1}(p-1)$.
3) Si m, n son primos entre sí, entonces $\Phi(mn) = \Phi(m)\Phi(n)$.
4) $\sum_{d \mid n} \Phi(d) = n$.

Por lo tanto, podemos finalizar este ejercicio diciendo que, si representamos por S al conjunto de todos los elementos de G que también generan el grupo cíclico G, se tiene

$$card(S) = \Phi(n). \clubsuit$$

Ex. 53 *Hallar el número de elementos de orden d de un grupo cíclico de orden n.*

$\equiv$

Como antes, d ha de ser un divisor de n. Del Ejercicio 48 sabemos que sólo hay un subgrupo de orden d. Sea H dicho subgrupo, que también es cíclico. Como todo elemento de orden d pertenece a H, del Ejercicio anterior, el número de elementos de orden d coincide con el número de elementos que generan H. Luego

$$\text{N° de elementos de orden } d = \Phi(d). \clubsuit$$

Ex. 54 *Sea u una raíz compleja n-ésima primitiva de la unidad. Sea v una raíz compleja m-ésima primitiva de la unidad. Si K designa el grupo multiplicativo formado por todos los números complejos de módulo unidad, hallar el subgrupo de K que generan u, v.*

$\equiv$

Recordemos que decir que u es una raíz compleja n-ésima primitiva de la unidad significa que u genera a todas las raíces n-ésimas de la unidad, es decir, si llamamos K_n al grupo multiplicativo formado por las raíces n-ésimas de la unidad, entonces $K_n = \langle u \rangle$. Análogamente se tiene que $K_m = \langle v \rangle$. Utilizando la forma polar de los números complejos sabemos que

$$K_n = \{1_0, 1_{\frac{2\pi}{n}}, ..., 1_{\frac{2(n-1)\pi}{n}}\}$$
$$K_m = \{1_0, 1_{\frac{2\pi}{m}}, ..., 1_{\frac{2(m-1)\pi}{m}}\}.$$

Veamos que $\langle u, v\rangle = K_n K_m$, siendo $K_n K_m = \{xy : x \in K_n, y \in K_m\}$.

[$\subset$] Si $x \in \langle u, v\rangle$, existen $p, q \in \mathbf{Z}$ tales que $x = u^p v^q$. Como $u \in K_n \rightarrow u^p \in K_n$ y $v \in K_m \rightarrow v^q \in K_m$, se tiene que $x = u^p v^q \in K_n K_m$.

[$\supset$] Si $w \in K_n K_m$, por definición, existen $x \in K_n$, $y \in K_m$ de modo que $w = xy$. Como $\langle u\rangle = K_n$, $\langle v\rangle = K_m$, existen $p, q \in \mathbf{Z}$ tales que $x = u^p$, $y = v^q$, de donde $w = xy = u^p v^q$ y se sigue que $w \in \langle u, v\rangle$. ♣

Ex. 55 *Siendo K_n, y K_m, los grupos multiplicativos formados por las raíces n-ésimas, y m-ésimas, respectivamente, de la unidad, describir el grupo $K_n \cap K_m$.*

≡

Llamando $d := mcd(n, m)$, veamos que $K_n \cap K_m = K_d$:

[$\subset$] Si $w \in K_n \cap K_m$, existen $i \in \{0, 1, ..., n-1\}$, $j \in \{0, 1, ..., m-1\}$ tales que $w = 1_{\frac{2i\pi}{n}} = 1_{\frac{2j\pi}{m}}$. Entonces, como los argumentos son ángulos posicionalmente equivalentes, existe un $k \in \mathbf{Z}$ tal que $\frac{2i\pi}{n} - \frac{2j\pi}{m} = 2k\pi$, de lo que $\frac{i}{n} - \frac{j}{m} = k \in \mathbf{Z}$. Como $0 \leq \frac{i}{n}, \frac{j}{m} < 1$, la resta $\frac{i}{n} - \frac{j}{m} \in]-1, 1[$, es decir $\frac{i}{n} - \frac{j}{m} \in]-1, 1[\cap \mathbf{Z} = \{0\}$. Por tanto, $\frac{i}{n} = \frac{j}{m}$. Además

$$d = mcd(n, m) \Rightarrow \exists p, q \in \mathbf{N} \text{ tal que } \left\{ \begin{array}{l} n = pd \\ m = qd \\ mcd(p, q) = 1 \end{array} \right\} \Rightarrow i = \frac{nj}{m} = \frac{pdj}{qd} = \frac{pj}{q}$$

$$\Rightarrow q \mid pj \Rightarrow q \mid j \Rightarrow \frac{j}{q} \in \mathbf{Z}.$$

Sea $h := \frac{j}{q} \in \mathbf{Z}$. Entonces, como $i = ph$,

$$w = 1_{\frac{2i\pi}{n}} = 1_{\frac{2ph\pi}{pd}} = 1_{\frac{2h\pi}{d}} \in K_d.$$

[$\supset$] Si $w \in K_d$, existe $0 \leq k \leq d-1$ tal que $w = 1_{\frac{2k\pi}{d}}$. Usando la terminología anterior, como $d = \frac{n}{p} = \frac{m}{q}$, se tiene que

$$\left. \begin{array}{rcl} w & = & 1_{\frac{2k\pi}{d}} = 1_{\frac{2kp\pi}{n}} \in K_n \\ w & = & 1_{\frac{2k\pi}{d}} = 1_{\frac{2kq\pi}{m}} \in K_m \end{array} \right\} \Rightarrow w \in K_n \cap K_m. \clubsuit$$

1.4. Subgrupos normales

Ex. 56 *Demostrar que un subgrupo H de un grupo G es normal si y sólo si todo cogrupo a la izquierda de H es igual a algún cogrupo a la derecha de H.*

≡

Recordemos que H es un subgrupo *normal* de G siempre que, $\forall x \in G$, $H^x := \{y \in G : xyx^{-1} \in H\} = H$. Observar que $H^x = x^{-1}Hx$.

[$\Rightarrow$] Supongamos que H es normal. Dado un cogrupo a la izquierda de H, xH, tenemos que $H = H^x = x^{-1}Hx$, lo que implica que $xH = Hx$.

[$\Leftarrow$] Queremos ver que H es normal. Si $x \in G$, como xH coincide con algún cogrupo a la derecha de H, existe un $y \in G$ tal que $xH = Hy$. Entonces $xHy^{-1} = H$, de lo que $xy^{-1} = xey^{-1} \in xHy^{-1} = H$; ello significa que $Hx = Hy$, por tanto $xH = Hy = Hx$ y, de la observación inicial, $H^x = x^{-1}Hx = H$. ♣

Ex. 57 *Demostrar que H es un subgrupo normal de G si y sólo si, $\forall x, y \in G$, $xy \in G$ implica que $x^{-1}y^{-1} \in G$.*

≡

[$\Rightarrow$] Supongamos que H es normal. Sean $x, y \in G$ tales que $xy \in H$. Entonces $y \in x^{-1}H = Hx^{-1}$, al ser normal. Por tanto, $yx \in H$, lo que implica que $x^{-1}y^{-1} = (yx)^{-1} \in H$.
[$\Leftarrow$] Para ver que H es normal, del ejercicio previo, basta demostrar que, si $x \in G$, entonces $H = x^{-1}Hx$: Si $y \in H$, entonces, como $x(x^{-1}y) = y \in H$, por hipótesis se tiene que $x^{-1}(x^{-1}y)^{-1} \in H$; pero $x^{-1}(x^{-1}y)^{-1} = x^{-1}y^{-1}x \in x^{-1}Hx$. Recíprocamente, si $y \in x^{-1}Hx$, existe $z \in H$ tal que $y = x^{-1}zx$, de donde, como $x(x^{-1}z) \in H$, por hipótesis $x^{-1}(x^{-1}z)^{-1} \in H$, de lo que $x^{-1}z^{-1}x \in H$; pero $x^{-1}z^{-1}x = (x^{-1}zx)^{-1} = y^{-1}$, luego $y^{-1} \in H$, y por tanto $y \in H$. ♣

Ex. 58 *Demostrar que todo subgrupo de índice 2 es siempre normal.*

≡

Sea H un subgrupo de G tal que $[G : H] = 2$ (recordemos que el índice de H es $[G : H] =$ *número de cogrupos izquierda, o derecha, de H*). Así, los cogrupos a la izquierda de H son $\{H, xH\}$, con $x \notin H$. Como se trata de un conjunto cociente de una relación de euivalencia, sabemos que $xH = G \setminus H$. Para ver que H es normal, basta con tomar $y \in G$ y demostrar que $yH = Hy$: Como yH es un cogrupo a la izquierda de H, tenemos dos posibilidades
Una. $yH = H$. Entonces $y \in H$, Por tanto $yH = H = Hy$.
Dos. $yH = xH = G \setminus H$. Obviamente, $y \notin H$. Así todo se reduce a ver que $Hy = G \setminus H$: Si $z \in Hy$, existe $h \in H$ tal que $z = hy$; entonces $y = h^{-1}z$ y, suponiendo que $z \in H$, tendríamos que $y \in H$, absurdo, luego $z \in G \setminus H$. Recíprocamente, si $z \in G \setminus H$, tenemos que $y^{-1}, z^{-1} \notin H$, y $y^{-1}H = G \setminus H = z^{-1}H$, de donde $yz^{-1} \in H$, con lo que $zy^{-1} \in H$, es decir, $z \in Hy$. ♣

Ex. 59 *Sean H y N subgrupos de G tales que N es normal en G. Demostrar que $H \cap N$ es normal en H.*

≡

Dado $x \in H$, hay que ver que $x(H \cap N) = (H \cap N)x$: Si $y \in x(H \cap N)$, existe $z \in H \cap N$ tal que $y = xz$; así $y = xz \in xN = Nx$, por lo que existe $u \in N$ de modo que $y = ux$; entonces $u = yx^{-1}$, pero, como $y = xz \in H$, tenemos que $u \in H \cap N$, es decir, $y = ux \in (H \cap N)x$. Recíprocamente, si $y \in (H \cap N)x$, sea $z \in H \cap N$ tal que $y = zx$; como antes, al ser N normal en G, $Nx = xN$ y existe un $u \in N$ tal que $y = zx = xu$; así $u = x^{-1}y \in N \cap H$, de donde $y = xu \in x(H \cap N)$. ♣

Ex. 60 *Sean N y N' subgrupos normales de G. Demostrar que NN' es también subgrupo normal de G.*

≡

Primero observemos que, al tratarse de subgrupos normales $NN' = N'N$: Si $x \in N$, $x' \in N'$, como $xx' \in xN' = N'x$, se tiene que $xx' \in N'N$, luego $NN' \subseteq N'N$. La inclusión recíproca es análoga.

Por tanto, del Ex. 35, podemos afirmar que NN' es un subgrupo de G. Veamos que es normal: Para ello, dado $x \in G$, veamos que $xNN' = NN'x$: Si $y \in xNN'$, existen $z \in N$, $z' \in N'$ tales que $y = xzz'$; entonces $y = (xz)z' \in (xz)N' = N'(xz)$, de donde existe un $z'' \in N'$ tal que $y = (xz)z' = z''(xz)$; pero, $xz \in xN = Nx$ implica que existe $u \in N$ tal que $xz = ux$; así, $y = z''(xz) = z''ux$ y como $z''u \in N'u = uN'$, existe $u' \in N'$ de modo que $z''u = u'u$; de lo que $y = z''ux = u'ux \in N'Nx$. La inclusión recíproca se demuestra de manera análoga. ♣

Ex. 61 *Sean H, K, N subgrupos de G tales que K es un subgrupo normal de H y N es normal en G. Demostrar que NK es normal en NH.*

≡

Primero observemos que $NK \subseteq NH$, ya que $K \subseteq H$, y además, como N es normal en G, del Ex.35, tenemos que NK y NH son subgrupos de G. Para ver que NK es normal en NH, todo consiste en tomar un elemento $x \in NH$ y comprobar que $xNK = NKx$: Sabemos que existen $a \in N$, $b \in H$ tales que $x = ab$. Demostramos la inclusión directa (la recíproca es similar)

Si $y \in xNK$, existen $u \in N$, $v \in K$ tales que $y = xuv = abuv$. Como $abu \in abN = Nab$, al ser N normal en G, existe $u' \in N$ tal que $abu = u'ab$. Pero, $bv \in bK = Kb$, ya que K es normal en H y $b \in H$, entonces existe $v' \in K$ tal que $bv = v'b$. Así, $y = abuv = u'abv = u'av'b = u'av'a^{-1}ab$; pero, $v'a^{-1} \in v'N = Nv'$, ya que N es normal en todo G, de lo que existe $u'' \in N$ tal que $v'a^{-1} = u''v'$ y, como $u'au'' \in N$, se tiene finalmente que

$$y = abuv = u'av'a^{-1}ab = u'au''v'ab = (u'au'')v'(ab) = ((u'au'')v')x \in NKx. \clubsuit$$

Ex. 62 *Demostrar que el centro Z_G de un grupo G es siempre normal.*

≡

Recordemos que el centro de un grupo G es el conjunto

$$Z_G := \{ x \in G : \forall y \in G,\ xy = yx \}.$$

Es fácil verificar que Z_G es un subgrupo de G. Para ver que es normal, dado $x \in G$, veamos que $xZ_G = Z_G x$: Si $y \in xZ_G$, existe un $z \in Z_G$ tal que $y = xz$; obviamente $y = xz = zx$, al pertenecer z al centro, por lo que $y = zx \in Z_G x$. La otra inclusión es totalmente análoga. ♣

Ex. 63 *Consideremos el conjunto*

$$Q = \{ e, a, a^2, a^3, b, ab, a^2b, a^3b \}.$$

Definiendo

$$a^4 = e, \quad a^2 = b^2, \quad aba = b,$$

se obtiene una estructura de grupo (el Grupo Quaternion). Demostrar que Q es un grupo no abeliano tal que todos sus subgrupos son normales (a esta propiedad se le llama ser "hamiltoniano", ya que fué Lord Hamilton quien inventó los "quaterniones").

≡

La tabla de Cayley de Q es la siguiente

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	e	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	e
a^2b	a^2b	ab	b	a^3b	e	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	e	a^3	a^2

Veamos que es un grupo no abeliano: Basta considerar los elementos a, b y ver que no conmutan

$$ba = a^3b \neq ab.$$

Para demostrar que todo subgrupo H de G es normal, consideramos una serie de casos posibles (casuística) según el valor del orden de H. Como $o(H) \in \{1, 2, 4, 8\}$, tenemos:
Uno. $o(H) = 1$. Entonces $H = \{e\}$ y claramente se trata de un subgrupo normal, pues el neutro conmuta con todo elemento del grupo.
Dos. $o(H) = 8$. Ahora, como antes, hay un único subgrupo de orden máximo, se trata de todo Q, y obviamente $xQ = Qx$, para todo $x \in Q$; es decir, el grupo total siempre es normal respecto de sí mismo.
Tres. $o(H) = 4$. En este caso el índice del subgrupo es $[G : H] = oQ)/o(H) = 2$ y ya vimos en el Ex.58 que todo subgrupo de índice 2 es normal.
Cuatro. $o(H) = 2$. Entonces sólo hay un subgrupo de este orden $H = \{e, a^2\}$ y puede verse mirando la tabla anterior que $xH = Hx$, $\forall x \in Q$. De hecho, el centro de Q es $Z_Q = \{e, a^2\}$, por lo que, del ejercicio anterior, también se desprende que este H es normal en Q. ♣

Ex. 64 *Demostrar que todo grupo no abeliano de orden 8 con un sólo elemento de orden 2 es isomorfo al Grupo Quaternion Q.*

$\equiv$

Sea $G = \{e, x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$, con x_2 siendo el único elemento de orden 2. Como G no es cíclico (al no ser abeliano), considerando el elemento x_1, tenemos que $o(x_1) \in \{2, 4\}$. Pero, como $x_1 \neq x_2$ y sólo hay un elemento de orden 2, se sigue que $o(x_1) = 4$. Entonces $x_1^4 = e$ y, como $e = (x_1^2)^2$, se tiene que $x_1^2 = x_2$. Supongamos (no supone restricción alguna) que: $x_3 = x_1^3$, $x_5 = x_1x_4$, $x_6 = x_1^2x_4$, $x_7 = x_1^3x_4$. Para tener que G es isomorfo a Q, todo se reduce a verificar que los elementos x_1, x_4 cumplen las tres condiciones definitorias de Q (ver ejercicio anterior). Es decir, como $G = \{e, x_1, x_1^2, x_1^3, x_4, x_1x_4, x_1^2x_4, x_1^3x_4\}$, tenemos que ver que

$$x_1^4 = e, \quad x_1^2 = x_4^2, \quad x_1x_4x_1 = x_4.$$

Ya vimos que $x_1^4 = e$. Vemos por exclusión que $x_4^2 = x_1^2$:

$$\left.\begin{array}{l} Si\ x_4^2 = x_7 \rightarrow x_4^2 = x_1^3x_4 \rightarrow x_4 = x_1^3 = x_3 \equiv Absurdo \\ Si\ x_4^2 = x_6 \rightarrow x_4^2 = x_1^2x_4 \rightarrow x_4 = x_1^2 = x_2 \equiv Absurdo \\ Si\ x_4^2 = x_5 \rightarrow x_4^2 = x_1x_4 \rightarrow x_4 = x_1 \equiv Absurdo \\ Si\ x_4^2 = x_4 \rightarrow x_4 = e \equiv Absurdo \\ Si\ x_4^2 = x_3 \rightarrow e = x_4^4 = x_3 = 2 \rightarrow x_3 = x_2 \equiv Absurdo \\ Si\ x_4^2 = x_1 \rightarrow e = x_4^4 = x_1^2 \rightarrow x_1 = x_2 \equiv Absurdo \end{array}\right\} \Rightarrow x_4^2 = x_2 = x_1^2.$$

Finalmente, vemos también por exclusión, que $x_1x_4x_1 = x_4$:

$$\begin{array}{l} Si\ x_1x_4x_1 = x_7 \rightarrow x_1x_4x_1 = x_1^3x_4 \rightarrow x_4x_1 = x_1^2x_4 = x_4^3 \rightarrow x_1 = x_4^2 = x_1^2 = x_2 \equiv Absurdo \\ Si\ x_1x_4x_1 = x_6 \rightarrow x_1x_4x_1 = x_1^2x_4 = x_4^3 \rightarrow x_1x_4x_1x_4 = e \rightarrow x_5^2 = e \rightarrow x_5 = x_2 \equiv Absurdo \\ Si\ x_1x_4x_1 = x_5 \rightarrow x_1x_4x_1 = x_1x_4 \rightarrow x_4x_1 = x_4 \rightarrow x_1 = e \equiv Absurdo \\ Si\ x_1x_4x_1 = x_3 \rightarrow x_1x_4x_1 = x_1^3 \rightarrow x_1x_4 = x_1^2 = x_2 \rightarrow x_5 = x_2 \equiv Absurdo \\ Si\ x_1x_4x_1 = x_2 \rightarrow x_1x_4x_1 = x_1^2 \rightarrow x_1x_4 = x_1 \rightarrow x_5 = x_1 \equiv Absurdo \\ Si\ x_1x_4x_1 = x_1 \rightarrow x_1x_4 = e \rightarrow x_5 = e \equiv Absurdo \\ Si\ x_1x_4x_1 = e \rightarrow x_1x_4 = x_1^3 \rightarrow x_5 = x_3 \equiv Absurdo \end{array}$$

Por tanto $x_1x_4x_1 = x_4$. ♣

Ex. 65 *Demostrar que $Q \ncong D_4$, es decir, que no son isomorfos.*

$\equiv$

Evidente: $Q = \{ e, a, a^2, a^3, b, ab, a^2b, a^3b \}$ sólo posee un elemento de orden 2, a^2, mientras que $D_4 = \{e, \rho, \rho^2, \rho^3, \sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma\}$, donde $\rho = (1234)$; $\sigma = (24)$, tiene 5 elementos de orden 2: $\rho^2, \sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma$. ♣

Ex. 66 *Sean H, K subgrupos normales de G tales que $H \cap K = \{e\}$. Demostrar que $HK \cong H \times K$.*

$\equiv$

Definimos $f : H \times K \rightarrow HK$ de modo que: $f(x, y) := xy$, $x \in H$, $y \in K$. Es evidente que f está bien definida. Veamos que es un isomorfismo de grupos.

f homomorfismo: Si $(a,b),(c,d) \in H \times K$, como $cb \in Hb = bH$, existe $c' \in H$ tal que $cb = bc'$; similarmente, como $cb \in cK = Kc$, existe $b' \in K$ tal que $cb = b'c$. Además, como $bc' = b'c$, se tiene que $c'c^{-1} = b^{-1}b' \in H \cap K = \{e\}$, de lo que $c'c^{-1} = e$ y $c = c'$, de donde $cb = bc$. Entonces

$$f((a,b)(c,d)) \;=\; f(ac,bd) \;=\; acbd \;=\; abcd \;=\; f(a,b)f(c,d).$$

f inyectiva: Si $(a,b),(c,d) \in H \times K$ son tales que $f(a,b) = f(c,d)$, entonces $ab = cd$, de donde $c^{-1}a = db^{-1} \in H \cap K = \{e\}$. Así, $c^{-1}a = e = db^{-1}$, por lo que $a = c$, $b = d$, es decir, $(a,b) = (c,d)$.
f sobre: Si $x \in HK$, existen $a \in H$, $b \in K$ tales que $x = ab$. Claramente, $(a,b) \in H \times K$ y $f(a,b) = ab = x$. ♣

Ex. 67 *Sean N_1, N_2, H_1, H_2 subgrupos de G tales que N_1 es normal en H_1 y N_2 es normal en H_2. Demostrar*

a) $N_1(H_1 \cap N_2)$ es normal en $N_1(H_1 \cap H_2)$.

b) $(H_1 \cap N_2)(H_2 \cap N_1)$ es normal en $H_1 \cap H_2$.

≡

a) Primero observemos que $N_1(H_1 \cap N_2) \subseteq N_1(H_1 \cap H_2)$. Ahora veamos que $N_1(H_1 \cap N_2)$ es subgrupo: Si $x, y \in N_1(H_1 \cap N_2)$, existen $a, c \in N_1$, $b, d \in H_1 \cap N_2$ de modo que $x = ab$, $y = cd$: Entonces $xy^{-1} = abd^{-1}c^{-1}$. Como $bd^{-1}c^{-1} \in bd^{-1}N_1 = N_1bd^{-1}$, ya que $bd^{-1} \in H_1$ y N_1 es normal en H_1, tenemos que existe $u \in N_1$ tal que $bd^{-1}c^{-1} = ubd^{-1}$. Así, $xy^{-1} = abd^{-1}c^1 = aubd^{-1} \in N_1(H_1 \cap N_2)$.

Para ver que $N_1(H_1 \cap N_2)$ es normal en $N_1(H_1 \cap H_2)$, si $x \in N_1(H_1 \cap H_2)$, hay que verificar la igualdad conjuntista $xN_1(H_1 \cap N_2) = N_1(H_1 \cap N_2)x$: Para la inclusión directa, sea $y \in xN_1(H_1 \cap N_2)$, exiten entonces $n_1 \in N_1$, $z \in H_1 \cap N_2$ tales que $y = xn_1z$. Pero, $xn_1 \in xN_1 = N_1x$, ya que $x \in H_1$ y N_1 es normal en H_1, de donde existe $n_1' \in N_1$ tal que $xn_1 = n_1'x$. Como $x \in N_1(H_1 \cap H_2)$, existen $m_1 \in N_1$, $v \in H_1 \cap H_2$ tales que $x = m_1v$. Luego, $xz = m_1vz \in m_1vN_2 = m_1N_2v$, ya que $v \in H_2$ y N_2 es normal en H_2, por tanto existe $z' \in N_2$ tal que $vz = z'v$, de lo que $z' = vzv^{-1} \in H_1$ y $z' \in H_1 \cap N_2$. Por tanto, $xz = m_1z'v \in N_1z'v = z'N_1v$, de lo que existe $m_1' \in N_1$ tal que $m_1z' = z'm_1'$, y, $xz = z'm_1'v$. Entonces

$$y \;=\; xn_1z \;=\; n_1'xz \;=\; n_1'z'm_1'v \;=\; n_1'z'm_1'm_1^{-1}m_1v \;=\; n_1'z'm_1'm_1^{-1}x.$$

Si llamamos $m_1'' := m_1'm_1^{-1} \in N_1$, entonces

$$y \;=\; n_1'z'm_1'm_1^{-1}x \;\in n_1'z'N_1x \;=\; n_1'N_1z'x \;\rightarrow\; \exists m_1''' \in N_1 \;/\; z'm_1'' = m_1'''z'.$$

Por lo tanto

$$y \;=\; n_1'z'm_1'm_1^{-1}x \;=\; n_1z'm_1''x \;=\; n_1'm_1'''z'x \;\in N_1(H_1 \cap N_2)x,$$

ya que $n_1m_1''' \in N_1$, $z' \in H_1 \cap N_2$.

La inclusión recíproca es análoga.

b) Aplicando el Ex.59, todo se reduce a ver que $H_1 \cap N_2$ y $H_2 \cap N_1$ son normales en $H_1 \cap H_2$. Para ello, observando que $H_1 \cap N_2$ es subgrupo de $H_1 \cap H_2$ y que N_2 es normal en H_2, aplicando el Ex.58 tenemos que $H_1 \cap N_2 = (H_1 \cap H_2) \cap N_2$ es normal en $H_1 \cap H_2$. De igual forma, ya que N_1 es normal en H_1, se tiene que $H_2 \cap N_1$ es normal en $H_1 \cap H_2$. ♣

Ex. 68 *Describir el grupo cociente* $\mathbf{Z}/m\mathbf{Z}$.

≡

En el grupo aditivo $\mathbf{Z}$ de los números enteros, $m\mathbf{Z}$ es el subgrupo formado por todos los múltiplos de m, es decir,

$$m\mathbf{Z} \;=\; \{\, x \in \mathbf{Z} \;:\; m \mid x \,\}.$$

Al estar en un grupo abeliano, es evidente que todo subgrupo es normal. Además, dados $x, y \in \mathbf{Z}$, la congruencia en módulo m, o sea, $x \equiv y \;(mod.m)$ es equivalente a que $x - y \in m\mathbf{Z}$, lo que es lo mismo que decir que los cogrupos (al ser el grupo abeliano, da igual por la izquierda que por la derecha) $x + m\mathbf{Z}$, $y + m\mathbf{Z}$ coinciden. Por tanto,

$$\mathbf{Z}/m\mathbf{Z} = \mathbf{Z}/\equiv (mod.m) = \{\overline{0} = m\mathbf{Z}, \overline{1} = 1{+}m\mathbf{Z}, \overline{2} = 2{+}m\mathbf{Z}, ..., \overline{m-1} = (m{-}1){+}m\mathbf{Z}\}.\ \clubsuit$$

Ex. 69 *Considerando* $\mathbf{Z}$ *como subgrupo del grupo aditivo de los números reales* $\mathbf{R}$, *demostrar que* $\mathbf{R}/\mathbf{Z}$ *es isomorfo a* K *(el Grupo Circular complejo).*

≡

El grupo circular complejo es el grupo multiplicativo dado por la circunferencia unidad compleja. Explícitamente

$$K \;=\; \{\, z \in \mathbf{C} \;:\; |\, z \,| = 1 \,\}.$$

Definimos $f : \mathbf{R} \to K$ tal que $f(t) := \mathrm{e}^{2\pi t i}$. Es decir, $f(t)$ es el complejo unitario $\cos 2\pi t + i \sin 2\pi t$.
$\underline{f \text{ bien definida}}$: Si $t \in \mathbf{R}$, es evidente que $f(t) = \cos 2\pi t + i \sin 2\pi t$ pertenece a K, ya que $|\cos 2\pi t + i \sin 2\pi t| = 1$.
$\underline{f \text{ homomorfismo}}$: Si $s, t \in \mathbf{R}$, $f(s+t) = \mathrm{e}^{2\pi(s+t)i} = \mathrm{e}^{2\pi s i} \cdot \mathrm{e}^{2\pi t i} = f(s) \cdot f(t)$.
$\underline{f \text{ sobre}}$: Si $z \in K$, como $|\, z \,| = 1$, sabemos que existe un $\alpha \in [0, 2\pi[$ tal que $z = \cos\alpha + i \sin\alpha$. Entonces, llamando $t := \frac{\alpha}{2\pi}$, tenemos que $f(t) = \mathrm{e}^{2\pi t i} = \mathrm{e}^{\alpha i} = \cos\alpha + i \sin\alpha = z$.
$\underline{Ker\ f \;=\; \mathbf{Z}}$: Recordemos que, ya que el neutro de K es 1, $Ker\ f = \{t \in \mathbf{R} :\ f(t) = 1\}$. Si $n \in \mathbf{Z}$, claramente $f(n) = \mathrm{e}^{2\pi n i} = \cos 2n\pi + i \sin 2n\pi \;=\; 1$, es decir, $n \in Ker\ f$. Recíprocamente, si $t \in \mathbf{R}$ es tal que $f(t) = 1$, entonces

$$\cos 2\pi t + i \sin 2\pi t = \mathrm{e}^{2\pi t i} = f(t) = 1 \Rightarrow \left\{ \begin{array}{l} \cos 2\pi t = 1 \\ \sin 2\pi t = 0 \end{array} \right\} \exists n \in \mathbf{Z} / 2\pi t = 0{+}2n\pi;\ t = n \in \mathbf{Z}.$$

Por tanto, aplicando la descomposición canónica de un homomorfismo de grupos

$$\mathbf{R}/\mathbf{Z} \;=\; \mathbf{R}/Ker\ f \;\cong\; f(\mathbf{R}) \;=\; K\ .\ \clubsuit$$

Ex. 70 *Demostrar que todo grupo cociente de un grupo cíclico es cíclico.*

≡

Sea H un subgrupo del grupo cíclico G. Sea $G = \langle\ x\ \rangle$. Todo consiste enver que $G/H = \langle xH \rangle$:

Si $y \in G$, entonces existe $n \in \mathbf{Z}$ tal que $y = x^n$, de lo que $yH = x^nH = (xH)^n \in \langle xH \rangle$. El recíproco es evidente. ♣

Ex. 71 *Sea H un subgrupo normal de G. Dado un elemento $a \in G$ de orden finito, demostrar que $o(aH) \mid o(a)$.*

≡

Supongamos que $o(a) = n$. Entonces

$$(aH)^n = (aH)(aH)\cdot \overset{(n)}{\cdots} \cdot(aH) = a^nH = eH = H.$$

Como H es el neutro del grupo cociente G/H, se sigue que $o(aH)$ es un divisor de n. ♣

Ex. 72 *Demostrar que si G/Z_G es cíclico, entonces G es abeliano.*

≡

Sabemos que el centro de G, Z_G, está formado por todos los elementos de G que conmutan con cualquier otro elemento de G. Por tanto, tiene sentido hablar del grupo cociente G/ZG. Supongamos que $G/Z_G = \langle xZ_G \rangle$. Para ver que G es abeliano, sean $y, z \in G$, entonces existen $n, m \in \mathbf{Z}$ tales que $yZ_G = (xZ_G)^n = x^nZ_G$, $zZ_G = (xZ_G)^m = x^mZ_G$. Así, como los cogrupos por la izquierda y por la derecha coinciden, se tiene que $x^{-n}y, zx^{-m} \in Z_G$, de donde

$$yz = y(zx^{-m})x^m = (zx^{-m})yx^m = zx^{-m}x^n(x^{-n}y)x^m = zx^{-m+n}x^m(x^{-n}y)$$
$$= zx^{-m+n+m-n}y = zy. \clubsuit$$

Ex. 73 *Sea H un subgrupo normal de G. Demostrar que G/H es abcliano si y sólo si, $\forall x, y \in G$, $xyx^{-1}y^{-1} \in H$.*

≡

[$\Rightarrow$] Suponiendo que G/H es abeliano. Si $x, y \in G$, como $Hxy = (Hx)(Hy) = (Hy)(Hx) = Hyx$, se tiene que $\exists h \in H$ tal que $xy = hyx$, de lo que $xyx^{-1}y^{-1} = (xy)(yx)^{-1} = h \in H$.

[$\Leftarrow$] Si ahora suponemos que se cumple que, $\forall x, y \in G$, $xyx^{-1}y^{-1} \in H$. Entonces, dados $Hx, Hy \in G/H$, tenemos que $(Hy)(Hx) = Hyx = (Hxyx^{-1}y^{-1})yx = Hxy(x^{-1}y^{-1}yx) = Hxy = (Hx)(Hy)$. ♣

Ex. 74 *Sea H un subgrupo normal de G. Sea K un subgrupo de G/H. Definimos $\widehat{K} := \{x \in G :\ xH \in K\}$. Demostrar que:*

a) $\widehat{K}$ es subgrupo de G y contiene a H.

b) $\widehat{K}$ es normal en G si y sólo si K es normal en G/H.

c) Deducir la existencia de una aplicación inyectiva entre la familia de los subgrupos normales de G/H y la de los subgrupos normales de G que contienen a H.

$\equiv$

a) Si $x, y \in \widehat{K}$, entonces veamos que $xy^{-1} \in \widehat{K}$: Evidente, $xy^{-1}H = (xH)(yH)^{-1} \in K$, ya que $xH, yH \in K$. Además, si $h \in H$, entonces es obvio que $hH = H \in K$, ya que H es el neutro de G/H, por tanto $h \in \widehat{K}$, es decir $H \subseteq \widehat{K}$.

b) [$\Rightarrow$] Supongamos que $\widehat{K}$ es normal en G. Para ver que K es normal en G/H, sea $xH \in G/H$, tenemos que probar que $(xH)K = K(xH)$: Si $yH \in K$, tenemos que $y \in \widehat{K}$, por lo que, como $x\widehat{K} = \widehat{K}x$, se tiene que existe $z \in \widehat{K}$ tal que $xy = zx$; de donde, como $zH \in K$, $(xH)(yH) = xyH = zxH = (zH)(xH) \in K(xH)$. La inclusión recíproca se demuestre de manera totalmente análoga.

[$\Leftarrow$] Supongamos ahora que K es normal en G/H. Para ver que $\widehat{K}$ es normal en G, dado $x \in G$, tenemos que verificar que $x\widehat{K} = \widehat{K}x$: Si $y \in \widehat{K}$, como $yH \in K$, $(xH)(yH) \in (xH)K = K(xH)$, así existe $zH \in K$ tal que $(xH)(yH) = (zH)(xH)$, es decir, $xyH = zxH$; por tanto, $xy \in zxH = zHx$, de donde, como $z \in \widehat{K}$ y $H \subseteq \widehat{K}$, se sigue que $xy \in zHx \subseteq \widehat{K}x$, como queríamos. La otra inclusión es análoga.

c) Representamos por $\mathcal{N}(G/H)$ y $\mathcal{N}(G, H)$ a las familias de los subgrupos normales de G/H y de subgrupos normales de G que contienen a H, respectivamente. Definimos la correspondencia $f : \mathcal{N}(G/H) \to \mathcal{N}(G, H)$ del siguiente modo, dado $K \in \mathcal{N}(G/H)$, establecemos $f(K) := \widehat{K}$, siendo $\widehat{K}$ el conjunto definido en el enunciado del ejercicio. Como resulta evidente que, para cada $K \in \mathcal{N}(G/H)$, siempre existe de manera única $\widehat{K}$, de los apartados b) y a) tenemos que f es una aplicación bien definida. Veamos que f es inyectiva: Sean $K_1, K_2 \in \mathcal{N}(G/H)$ tales que $f(K_1) = f(K_2)$. Entonces $\widehat{K_1} = \widehat{K_2}$, de donde, dado $xH \in K_1$, por definición de $\widehat{K_1}$, $x \in \widehat{K_1}$, consecuentemente $x \in \widehat{K_2}$, es decir, $xH \in K_2$, lo que demuestra que $K_1 \subseteq K_2$. Análogamente se ve que $K_2 \subseteq K_1$, con lo que $K_1 = K_2$ y f es pues inyectiva. ♣

Ex. 75 *Sean H un subgrupo normal de G y H' un subgrupo normal de G'. Demostrar que:*

a) $H \times H'$ es subgrupo normal de $G \times G'$.

b) $(G \times G')/(H \times H') \cong G/H \times G'/H'$.

$\equiv$

a) Como en general $H \times H'$ es subgrupo de $G \times G'$, veamos que, si $(x, x') \in G \times G'$, $(x, x')(H \times H') = (H \times H')(x, x')$: Si $(y, y') \in H \times H'$, entonces $xy \in xH = Hx$, de donde existe $z \in H$ tal que $xy = zx$; análogamente, existe $z' \in H'$ tal que $x'y' = z'x'$; así $(x, x')(y, y') = (xy, x'y') = (zx, z'x') = (z, z')(x, x')$; es decir $(x, x')(H \times H') \subseteq (H \times H')(x, x')$. La inclusión recíproca es análoga.

b) Definimos $f : (G \times G')/(H \times H') \to G/H \times G'/H'$ del siguiente modo: Si $(x, x')(H \times H') \in (G \times G')/(H \times H')$, sea $f((x, x')(H \times H')) := (xH, x'H')$.

f bien definida: Para verlo hay que demostrar que no depende del representante elegido, es decir, si $(x, x')(H \times H') = (y, y')(H \times H')$, se tiene que

$$(x^{-1}y, x'^{-1}y') = (x, x')^{-1}(y, y') \in H \times H' \Rightarrow \left\{ \begin{array}{l} x^{-1}y \in H \\ x'^{-1}y' \in H' \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} xH = yH \\ x'H' = y'H' \end{array} \right\}$$

$$\Rightarrow f((x, x')(H \times H')) = (xH, x'H') = (yH, y'H') = f((y, y')(H \times H')).$$

f homomorfismo: Dados $(x,x')(H\times H'),(y,y')(H\times H')\in (G\times G')/(H\times H')$

$$f((x,x')(H\times H')(x,x')(H\times H')) = f((xy,x'y')(H\times H')) = (xyH,x'y'H')$$
$$= ((xH)(yH),(x'H')(y'H')) = (xH,x'H')(yH,y'H')$$
$$= f((x,x')(H\times H'))f((y,y')(H\times H')).$$

f inyectiva: Como ya sabemos que f es homomorfismo de grupos, todo consiste en ver que, si $(x,x')(H\times H')\in (G\times G')/(H\times H')$ es tal que $f((x,x')(H\times H'))=(H,H')$, entonces $(x,x')(H\times H')=H\times H'$:

$$f((x,x')(H\times H'))=(H,H')\Rightarrow (xH,x'H')=(H,H')\Rightarrow \left\{\begin{array}{l} xH=H\to x\in H \\ x'H'=H'\to x'\in H' \end{array}\right\}$$
$$\Rightarrow (x,x')(H\times H')=H\times H'.$$

f sobre: Si $(xH,x'H')\in G/H\times G'/H'$, es evidente que $(x,x')(H\times H')\in (G\times G')/(H\times H')$ y además $f((x,x')(H\times H'))=(xH,x'H')$. ♣

Ex. 76 *Consideramos el grupo dihédrico* $D_6=\{e,\rho,\rho^2,\rho^3,\rho^4,\rho^5,\sigma,\rho\sigma,\rho^2\sigma,\rho^3\sigma,\rho^4\sigma,\rho^5\sigma\}$, *siendo* $\rho:=(123456)$ *y* $\sigma:=(26)(35)$. *Calcular el normalizador de* $\{\rho\}$, *de* $\{\sigma\}$ *y de* $\langle\ \rho\ \rangle$.

≡

Recordemos primero que, en un grupo G, si $A\subseteq G$, $x\in G$, por A^x se representa el subconjunto de G dado por

$$A^x = \{\ x^{-1}ax\ :\ a\in A\ \}.$$

Entonces se define el *normalizador de* A como

$$N(A) = \{\ x\in G\ :\ A^x=A\ \}.$$

Veamos que $N(\{\rho\})=\langle\ \rho\ \rangle=\{e,\rho,\rho^2,\rho^3,\rho^4,\rho^5\}$:
[$\supset$] Evidente, pues $\forall i=0,1,2,3,4,5$,

$$\{\rho\}^{\rho^i} = (\rho^i)^{-1}\{\rho\}\rho^i = \{\rho^{6-i}\rho\rho^i\} = \{\rho\}.$$

[$\subset$] Sea $s\in N(\{\rho\})$. Supongamos que $s\notin\langle\ \rho\ \rangle$. Entonces, para algún $i\in\{0,1,2,3,4,5\}$ se tiene que $s=\rho^i\sigma$. Así, como $(\rho^i\sigma)^{-1}=\rho^i\sigma$, y $\sigma\rho^i=\rho^{6-i}\sigma$,

$$s^{-1}\rho s=(\rho^i\sigma)^{-1}\rho(\rho^i\sigma)=\rho^i(\sigma\rho)\rho^i\sigma=\rho^i\rho^5(\sigma\rho^i)\sigma=\rho^{i+5}\rho^{6-i}\sigma^2=\rho^{11}=\rho^5\neq\rho.\ \textit{Absurdo}$$

Veamos que $N(\{\sigma\})=\{e,\rho^3,\sigma,\rho^3\sigma\}$:
Para $i\in\{0,1,2,3,4,5\}$

$$\rho^i\in N(\{\sigma\})\leftrightarrow(\rho^i)^{-1}\sigma\rho^i=\sigma\leftrightarrow\rho^{6-i}\rho^{6-i}\sigma=\sigma\leftrightarrow\rho^{12-2i}=e\leftrightarrow 12-2i\equiv 0\ (mod,6)$$
$$\leftrightarrow i\in\{0,3\}\leftrightarrow\rho^i\in\{e,\rho^3\}.$$

$$\rho^i\sigma \in N(\{\sigma\}) \leftrightarrow (\rho^i\sigma)^{-1}\sigma\rho^i\sigma = \sigma \leftrightarrow \rho^i\sigma\sigma\rho^i\sigma = \sigma \leftrightarrow \rho^{2i} = e \leftrightarrow 2i \equiv 0 \ (mod,6)$$
$$\leftrightarrow i \in \{0,3\} \leftrightarrow \rho^i\sigma \in \{\sigma, \rho^3\sigma\}.$$

Veamos que $N(\langle\ \rho\ \rangle) = D_6$: Obviamente sólo tenemos que probar la inclusión recíproca. Si $i, j \in \{0,1,2,3,4,5\}$

$$(\rho^i\sigma)^{-1}\rho^j\rho\sigma \ = \ \rho^i\sigma\rho^j\rho^i\sigma \ = \ \rho^i\sigma\rho^{i+j}\sigma \ = \ \rho^i\rho^{6-i-j}\sigma\sigma \ = \ \rho^{6-j} \ \in \ \langle\ \rho\ \rangle \ \Rightarrow \ \rho^i\sigma \in N(\langle\ \rho\ \rangle).$$

Es evidente que $\rho^i \in \langle\ \rho\ \rangle \ \subseteq \ N(\langle\ \rho\ \rangle) = D_6$, $0 \leq i \leq 5$. ♣

Ex. 77 *Sea H el subgrupo del grupo simétrico Σ_n formado por todas las permutaciones que dejan a n invariante.*

1) Hallar el normalizador de H.

2) Indicar todos los conjugasdos de H en Σ_n.

≡

Tenemos que

$$H \ = \ \{\ s \in \Sigma_n \ : \ s(n) = n\ \}.$$

1) Si $n = 2$, entonces es evidente que $H = \{\ e\ \}$, por lo que $N(H) = \Sigma_2$. Supongamos que $n \geq 3$ y veamos que $N(H) = H$: Como en general $H \subseteq N(H)$, demostramos la inclusión recíproca. Sea $s \in N(H)$, entonces, $\forall t \in H$, se tiene que $s^{-1}ts \in H$. Si $s \notin H$, entonces, para algún $i \in \{1,2,...,n-1\}$, $s(n) = i$. Al ser $n \geq 3$, podemos tomar un $j \in \{1,2,...,n\}$, $j \neq i$, $j \neq n$, de modo que, considerant la transposición $t := (i,j)$, tenemos que

$$\left.\begin{array}{l} t \in H \ (ya\ que\ t(n) = n) \\ s^{-1}ts(n) = s^{-1}t(i) = s^{-1}(j) \neq n \ (pues\ s^{-1}(j) = n \rightarrow s(n) = j,\ absurdo) \end{array}\right\} \ s^{-1}ts \notin H.,$$

lo que contradice nuestra observación inicial. Así pues, resumiendo

$$N(H) \ = \ \left\{\begin{array}{ll} \Sigma_2, & si \ \ n = 2, \\ H, & si \ \ n \geq 3\ . \end{array}\right.$$

2) Dado $1 \leq i \leq n$, sea $H_i := \{s \in \Sigma_n \ : \ s(i) = i\}$. Claramente, los H_i son subgrupos de Σ_n y $H = H_n$. Veamos que los únicos subgrupos de Σ_n conjugados de H son dichos H_i, $1 \leq i \leq n$:

Sea N un subgrupo de Σ_n conjugado de H. Por definición de subgrupo conjugado, existe $s \in \Sigma_n$ tal que $N = s^{-1}Hs$. Sea $i := s^{-1}(n)$ y veamos que $N = H_i$: Si $t \in N$, existe $h \in H$ tal que $t = s^{-1}hs$, de donde $t(i) = s^{-1}hs(i) = s^{-1}h(n) = s^{-1}(n) = i$, es decir, $t \in H_i$. Recíprocamente, si $t \in H_i$, entonces

$$sts^{-1}(n) = st(i) = s(i) = n \ \rightarrow \ \ sts^{-1} \in H \ \rightarrow \ t \in s^{-1}Hs \ = \ N. \ ♣$$

Nota 6 De lo que acabamos de ver en el apartado 1) podríamos haber deducido el número de conjugados de H del siguiente modo: Para $n \geq 3$,

$$N\acute{u}mero\ de\ conjugados\ de\ H \ = \ [\Sigma_n : N(H)] \ = \ [\Sigma_n : H] \ = \ \frac{n!}{(n-1)!} \ = \ n.$$

Ex. 78 *Demostrar que:* $\forall a \in G, \forall S \subseteq G, \quad N(S^a) = N(S)^a$.

$\equiv$

Recordemos que $S^a = a^{-1}Sa$.

[$\subset$] Si $x \in N(S^a)$,

$$(S^a)^x = S^a \rightarrow x^{-1}S^a x = x^{-1}a^{-1}Sax = a^{-1}Sa \rightarrow ax^{-1}a^{-1}Saxa^{-1} = S.$$

Llamando $y := axa^{-1}$,

$$S^y = y^{-1}Sy = ax^{-1}a^{-1}Saxa^{-1} = S \rightarrow y \in N(S) \rightarrow x = a^{-1}ya \in a^{-1}N(S)a = N(S)^a.$$

[$\supset$] Si $x \in N(S)^a$, existe $y \in N(S)$ tal que $x = a^{-1}ya$. Todo se reduce a ver que $(S^a)^x = S^a$: Como $y \in N(S)$, tenemos

$$x^{-1}S^a x = x^{-1}a^{-1}Sax = a^{-1}y^{-1}aa^{-1}Saa^{-1}ya = a^{-1}y^{-1}Sya = a^{-1}Sa = S^a \rightarrow x \in N(S^a).\clubsuit$$

Ex. 79 *Sea S un subconjunto no vacío del grupo G, no trivial, tal que tiene exactamente dos conjugados. Demostrar que G admite un subgrupo propio normal.*

$\equiv$

Puesto que $[G : N(S)] = 2$, de un problema visto anteriormente sabemos que el normalizador de S, $N(S)$, es un subgrupo normal de G. Por tanto, todo consiste en ver que $N(S)$ es un subgrupo propio, i.e., $N(S) \neq \{e\}$, $N(S) \neq G$: Obviamente, $N(S) \neq G$, de lo contrario $[G : N(S)] = [G : G] = 1$. Además, $N(S) \neq \{e\}$, si no $S = \{e\}$, lo que implicaría que $N(S) = G$, es decir, $G = \{e\}$, lo que contradice la no trivialidad de G. $\clubsuit$

Ex. 80 *Sea G un grupo finito. Sea H un subgrupo propio de G. Demostrar que G contiene más elementos que la unión de todos los conjugados de H.*

$\equiv$

Al estar en un grupo finito, el número de conjugados de H es finito, sean $x_1^{-1}Hx_1$, $x_2^{-1}Hx_2$, ..., $x_n^{-1}Hx_n$ los distintos conjugados de H. Como $n = [G : N(H)]$, tenemos que $o(G) = o(N(H)n$. Consideramos dos posibilidades:

Una. $n = 1$. Entonces H es el único conjugado de H y , como H es un subconjunto propio de G, queda claro que $o(G) > o(H)$, es decir, G tiene más elelmentos que H, que es la unión de los conjugados de H.

Dos. $n > 1$. Aquí, como $e \in \cap_{i=1}^n x_i^{-1}Hx_i$, se tiene, observando que los conjugados de H, al ser isomorfos, tiene el mismo cardinal, el de H,

$$card(\cup_{i=1}^n x_i^{-1}Hx_i) \leq n \cdot o(H) - (n-1) \leq n \cdot o(N(H)) - (n-1) = o(G) - (n-1) < o(G),$$

ya que $n - 1 > 0$. $\clubsuit$

Ex. 81 *Demostrar que, para cualquier $n \geq 3$, el centro del grupo simétrico Σ_n es trivial.*

$\equiv$

Recordemos que, dado un grupo G, su *centro* se define como el subconjunto (puede verse que es un subgrupo) formado por todos los elementos de G que conmutan con todos los elementos de G. Explícitamente

$$Z_G \;=\; \{\, x \in G \;:\; xy = yx,\;\; \forall y \in G \,\}.$$

Observar primero que, para $n = 2$: $\Sigma_2 = \{e, (12)\}$, por lo que $Z_{\Sigma_2} = \Sigma_2$. Supongamos que $n \geq 3$ y veamos que $Z_{\Sigma_n} = \{e\}$. Razonando por reduccción al absurdo, sea $s \in Z_{\Sigma_n}$ tal que $s \neq e$. Entonces $\exists i \neq j \in \{1, 2, ..., n\}$ tales que $s(i) = j$. Al ser $n > 2$, podemos encontrar un $k \in \{1, 2, ..., n\} \setminus \{i, j\}$. Consideremos la permutación $(j, k) \in \Sigma_n$, es decir, la biyección de $\{1, 2, ..., n\}$ en sí mismo que intercambia j y k dejando invariantes a los demás elementos. Entonces

$$\left.\begin{array}{rcl} s(j,k)(i) & = & s(i) \;=\; j \\ (j,k)s(i) & = & (j,k)(j) \;=\; k \end{array}\right\} \;\Rightarrow\; s(j,k) \;\neq\; (j,k)s\;,$$

lo que es absurdo, ya que $s \in Z_{\Sigma_n}$. ♣

Ex. 82 *Hallar el centro del grupo dihédrico D_n.*

$\equiv$

Recordemos que el grupo dihédrico $D_n = \{e, \rho, \rho^2, ..., \rho^{n-1}, \sigma, \rho\sigma, ..., \rho^{n-1}\sigma\}$, donde, suponiendo que estamos permutando los vértices de un polígono regular de n lados, ρ es el giro de ángulo $\frac{2\pi}{n}$ y σ es una simetría axial. Como $D_n = \langle\, \rho,\; \sigma \,\rangle$, está claro que $s \in Z_{D_n}$ si y sólo si s conmuta con ρ y con σ. Así, distinguimos dos posibilidades:
Una. n es impar. Veamos que en este caso $Z_{D_n} = \{e\}$: Sea $s = \rho^i\sigma^j$, con $i \in \{0, 1, ..., n-1\}$, $j \in \{0, 1\}$, tal que $s \in Z_{D_n}$.

$$\left.\begin{array}{l} Si\;\; j = 0: \;\; s = \rho^i; \;\; s\sigma = \sigma s \to \rho^i\sigma = \sigma\rho^i = \rho^{n-i}\sigma \to \rho^i = \rho^{n-i} \to i \equiv n - i \;(mod.n) \\ Si\;\; j = 1: \;\; s = \rho^i\sigma; \;\; s\rho = \rho s \to \rho^i\sigma\rho = \rho\rho^i\sigma \to \rho^{n+i-1}\sigma = \rho^{i+1}\sigma \to \rho^{n+i-1} = \rho^{i+1} \end{array}\right\} \Rightarrow$$

$$\left\{\begin{array}{l} \to n|\; n - 2i \overset{n\;impar}{\to} n|\; i \overset{0\leq i<n}{\to} i = 0 \to \;\; s = e \\ \to n + i - 1 \equiv i + 1 \;(mod.n) \to n|\; n - 2 \to \left\{\begin{array}{l} n = 1 \to D_n = \{e\} = Z_{D_n} \\ n = 2.\; \textit{Absurdo, pues n es impar.} \end{array}\right. \end{array}\right.$$

Por tanto, $s = e$.
Dos. n es par. Veamos que en este caso $Z_{D_n} = \{e, \rho^{\frac{n}{2}}\}$: Sea $s = \rho^i\sigma^j$, con $i \in \{0, 1, ..., n-1\}$, $j \in \{0, 1\}$, tal que $s \in Z_{D_n}$.

$$\left.\begin{array}{l} Si\;\; j = 0: \;\; s = \rho^i; \;\; s\sigma = \sigma s \to \rho^i\sigma = \sigma\rho^i = \rho^{n-i}\sigma \to \rho^i = \rho^{n-i} \to i \equiv n - i \;(mod.n) \\ Si\;\; j = 1: \;\; s = \rho^i\sigma; \;\; s\rho = \rho s \to \rho^i\sigma\rho = \rho\rho^i\sigma \to \rho^{n+i-1}\sigma = \rho^{i+1}\sigma \to \rho^{n+i-1} = \rho^{i+1} \end{array}\right\} \Rightarrow$$

$$\left\{\begin{array}{l} \to n|\; n - 2i \to n|\; 2i \overset{0\leq i<n}{\to} 2i \in \{0, n\} \to i \in \{0, \frac{n}{2}\} \to s = \rho^i \in \{e, \rho^{\frac{n}{2}}\} \\ \to n + i - 1 \equiv i + 1 \;(mod.n) \to n|\; n - 2 \to \left\{\begin{array}{l} n = 1.\; \textit{Absurdo, pues n es par} \\ n = 2 \to \{e, \rho^{\frac{n}{2}}\} = \{e, \rho\} = D_n = Z_{D_n}. \end{array}\right. \end{array}\right. \;\clubsuit$$

Ex. 83 *Hallar el centro del grupo quaternion Q.*

$\equiv$

Recordemos que el grupo quaternion es $Q = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, con $a^4 = e$, $a^2 = b^2$, $aba = b$. Veamos que $Z_Q = \{e, a^2\}$:
$[\supset]$ Es evidente que el neutro e siempre pertenece al centro de un grupo. Para ver que $a^2 \in Z_Q$, como $Q = \langle a, b \rangle$, todo se reduce a ver que a^2 conmuta con b:

$$a^2b = b^2b = b^3 = bb^2 = ba^2.$$

$[\subseteq]$ Sea $x \in Z_Q$, entonces $\exists i \in \{0,1,2,3\}$, $\exists j \in \{0,1\}$ tales que $x = a^ib^j$. Si $j = 1$, entonces, como $xa = ax$, tendríamos

$$xa = ax \rightarrow a^iba = aa^ib = a^{i+1}b = a^{i+2}ba \rightarrow a^i = a^{i+2} \rightarrow e = a^2. \textit{ Absurdo}$$

Por tanto, $x = a^i$. Ahora, como $xb = bx$, se tiene, ya que $ba^i = a^{4-i}b$,

$xb = bx \rightarrow a^ib = ba^i = a^{4-i}b \rightarrow a^i = a^{4-i} \rightarrow 4|\, 4-2i \overset{0\leq i<4}{\Longrightarrow} i \in \{0,2\} \rightarrow x = a^i \in \{e, a^2\}$. ♣

Ex. 84 *Separar los elementos del grupo quaternion Q en clases de conjugación, comprobando la ecuación de dichas clases.*

$\equiv$

Recordemos que, si x es un elemento de un grupo G, por *clase de conjugación* de x se entiende el subconjunto

$$C_x := \{\, yxy^{-1} : y \in G \,\}.$$

Así

$C_e = \{xex^{-1} : x \in Q\} = \{e\}$ *(cierto en general)*
$C_a = \{xax^{-1} : x \in Q\} = \{a^iaa^{4-i}, a^iba(a^ib)^{-1} = a^ibab^{-1}a^{4-i} = a^3 : 0 \leq i \leq 3\} = \{a, a^3\}$
$C_{a^2} = \{xa^2x^{-1} : x \in Q\} = \{a^2\}$, *pues* $a^2 \in Z_Q$
$C_b = \{xbx^{-1} : x \in Q\} = \{b, a^2b\}$
$C_{ab} = \{xabx^{-1} : x \in Q\} = \{ab, a^3b\}$.

La ecuación de las clases de conjugación de un grupo G es

$$o(G) = o(Z_G) + \sum_{x \notin Z_G} card(C_x).$$

Por tanto, como $Z_Q = \{e, a^2\}$,

$$8 = o(Q) = o(Z_q) + card(C_a) + card(C_b) + card(C_{ab}) = 2 + 2 + 2 + 2. \clubsuit$$

Ex. 85 *Demostrar que todo grupo de orden p^2, con p número primo, es abeliano.*

$\equiv$

Sea G un grupo tal que $o(G) = p^2$, donde p es un número primo. Haciendo uso de la ecuación de las clases de conjugación de G, existen $x_1, x_2, ..., x_n \in G \setminus Z_G$ de modo que

$$p^2 = o(G) = o(Z_G) + card(C_{x_1}) + card(C_{x_2}) + ... + card(C_{x_n})$$

$$= o(Z_G) + [G : N(x_1)] + [G : N(x_2)] + ... + [G : N(x_n)],$$

donde $[G : N(x_i)]$ es el índice del subgrupo $N(x_i)$, el normalizador de x_i, en G. Antes de seguir, para comprender lo anterior veamos que $card(C_x) = [G : N(x)]$: Para ello definimos la aplicación $f : C_x \to G/N(x)$ tal que, si $yxy^{-1} \in C_x$, $f(yxy^{-1}) := y + N(x)$. Es evidente que f está bien definida. Para tener la igualdad deseada todo se reduce a ver que f es biyectiva: Si $f(yxy^{-1} = f(zxz^{-1})$, entonces

$$y + N(x) = z + N(x) \ \to \ y^{-1}z \in N(x) \ \to \ (yxy^{-1})(zxz^{-1})^{-1} = yxy^{-1}zx^{-1}z^{-1}$$

$$= [y^{-1}z \ commuta \ con \ x] = yy^{-1}zxx^{-1}z^{-1} = e \ \to \ yxy^{-1} = zxz^{-1} \ \Rightarrow \ f \ es \ inyectiva.$$

Finalmente, si $y + N(x) \in G/N(x)$, está claro que $y + N(x) = f(yxy^{-1})$, con lo que f también es sobre.

Para cada $i = 1, 2, ..., n$, $card(C_{x_i}) = [G : N(x_i)]$ es un divisor de $o(G) = p^2$. Como $[G : N(x_i)] < o(G)$ (ya que si no fuese así se tendría que, de la ecuación de conjugación, $o(Z_G) = 0$, que es absurdo), se tiene que $card(C_{x_i})|\ p$. Pero $card(C_{x_i}) = [G : N(x_i)] > 1$, de lo contrario $G : N(x_i)] = 1$ implicaría que $G = N(x_i)$, esw decir $x_i \in Z_G$, lo que no es así. Por tanto, $crad(C_{x_i}) = [G : N(x_i)] = p$. Entonces

$$o(Z_G) = p^2 - p - p - ... - p = p^2 - np = p(p - n) \ \to \ p|\ o(Z_G).$$

Ahora bien, como $o(Z_G)$ es un divisor de $o(G) = p^2$, tenemos dos posibilidades:
Una. $o(Z_G) = p^2$. Claramente G es abeliano, ya que $G = Z_G$.
Dos. $o(Z_G) = p$. Entonces, como Z_G es un subgrupo normal de G, se tiene que G/Z_G es un grupo y $o(G/Z_G) = \frac{p^2}{p} = p \ \equiv \ primo$ implica que G/Z_G es un grupo cíclico. De un problema anterior, el Ex. 71, sabemos que en este caso G es abeliano. Pero entonces $Z_G = G$ y $o(Z_G) = o(G) = p^2$, lo que nos dice que esta posibilidad es absurda. ♣

1.5. Grupos actuando sobre conjuntos

Ex. 86 *Explicar cómo actúa el grupo simétrico Σ_n sobre un conjunto de n elementos.*

$\equiv$

Recordemos que se dice que un grupo G *actúa* sobre un conjunto X siempre que existe una aplicación de la forma $* : G \times X \to X$ (la *actuación*) que cumple:

a) $\forall g_1, g_2 \in G, \forall x \in X, \ g_1 * (g_2 * x) = (g_1 g_2) * x.$

b) $\forall x \in X, \ e * x = x.$

Cuando se tiene la actuación de un grupo G sobre un conjunto X, se dice que G es un *grupo de transformaciones* sobre X.

La actuación del grupo simétrico Σ_n sobre $X = \{x_1, x_2, ..., x_n\}$ es la natural. es decir

$$\forall s \in \Sigma_n, \quad \forall i \in \{1, 2, ..., n\}. \quad s * x_i \ = \ x_{s(i)}.$$

Veamos que se trata de una actuación:

a) Si $s_1, s_2 \in \Sigma_n$, $i \in \{1, 2, ..., n\}$,

$$s_1 * (s_2 * x_i) \ = \ s_1 * x_{s_2(i)} \ = \ x_{s_1(s_2(i))} \ = \ x_{(s_1 s_2)(i)} \ = \ (s_1 s_2) * x_i.$$

b) $\forall i \in \{1, 2, ..., n\}$, $e * x_i \ = \ x_{e(i)} \ = \ x_i$. ♣

Ex. 87 *Sea G un grupo de transformaciones sobre un conjunto X. Consideramos el subconjunto $G_0 := \{\ g \in G \ : \ g * x = x, \ \forall x \in X\}$. Demostrar que G_0 es un subgrupo normal de G.*

≡

Veamos primero que G_0 es un subgrupo de G: Si $g, h \in G_0$, entonces, $\forall x \in X$,

$$\left.\begin{array}{l} (gh) * x \ = \ g * (h * x) \ = \ g * x \ = \ x \\ g^{-1}x \ = \ g^{-1}(g * x) \ = \ (g^{-1}g) * x \ = \ e * x \ = \ x \end{array}\right\} \ \Rightarrow \ \left\{\begin{array}{l} gh \in G_0 \\ g^{-1} \in G_0. \end{array}\right.$$

Para demostrar que G_0 es un subgrupo normal de G, tomamos un arbitrario $g \in G$ y tenemos que probar que $gG_0 = G_0 g$, es decir, que $gG_0g^{-1} = G_0$:

$$\forall h \in gG_0g^{-1} \rightarrow \ \exists u \in G_0 \ / \ h = gug^{-1}.$$

Entonces, $\forall x \in X$

$$h * x = (gug^{-1}) * x = g * (u * (g^{-1} * x)) = g * (g^{-1} * x) = (gg^{-1}) * x = e * x = x \rightarrow h \in G_0$$

$$\Rightarrow gG_0g^{-1} \subseteq G_0.$$

La inclusión recíproca se demuestra análogamente. ♣

Ex. 88 *Un grupo de transformaciones G se dice que actúa efectivamente sobre el conjunto X cuando, además de actuar sobre X, se cumple que: Si $g \in G$ es tal que $g * x = x$, $\forall x \in X$, entonces $g = e$ (es decir, cuando el único elemento del grupo que deja invariantes a todos los elementos del conjunto es el neutro). Demostrar que para cualquier grupo de transformaciones G sobre un conjunto X, si G_0 es el subgrupo normal de G introducido en el ejercicio previo, se tiene que el grupo cociente G/G_0 actúa efectivamente sobre X.*

≡

Observemos que tiene sentido hablar del grupo cociente G/G_0, ya que G_0 es un subgrupo normal de G. Definimos la siguiente actuación de G/G_0 sobre X: $\bullet : G/G_0 \times X \rightarrow X$ tal que, si $g \in G$, $x \in X$, entonces $gG_0 \bullet x := g * x$. Tenemos que ver lo siguiente

• bien definida: Sean $g_1, g_2 \in G$ tales que $g_1G_0 = g_2G_0$, dado $x \in X$

$$g_1^{-1}g_2 \in G_0 \ \rightarrow \ x = (g_1^{-1}g_2) * x = g_1^{-1} * (g_2 * x) \ \rightarrow \ g_1 * x = g_2 * x \ \rightarrow \ g_1G_0 \bullet x = g_2G_0 \bullet x.$$

• es una actuación sobre X: Sean $g_1, g_2 \in G$, $x \in X$,

$$g_1G_0 \bullet (g_2G_0 \bullet x) = g_1G_0 \bullet (g_2 * x) = g_1 * (g_2 * x) = (g_1g_2) * x = (g_1G_0g_2G_0) \bullet x$$
$$G_0 \bullet x = eG_0 \bullet x = e * x = x.$$

• es una actuación efectiva: Sea $g \in G$ tal que, $\forall x \in X$, $gG_0 \bullet x = x$. Entonces, recordando la definición del subgrupo G_0,

$$x = gG_0 \bullet x = g * x, \ \forall x \in X \ \Rightarrow \ \ g \in G_0 \ \Rightarrow \ \ gG_0 = G_0. \ \clubsuit$$

Ex. 89 *Demostrar que un grupo G actúa efectivamente sobre el conjunto de los cogrupos a la izquierda, que indicamos por $(G/H)_i$, si y sólo si $\cap_{x \in G} H^x = \{e\}$.*

$\equiv$

[$\Rightarrow$] Supongamos que $*$ es una actuación efectiva del grupo G sobre $(G/H)_i$. Sea $y \in \cap_{x \in G} H^x$. Entonces, $\forall x \in G$, $y \in H^{x^{-1}} = xHx^{-1}$, por lo que existe $z \in H$ tal que $y = xzx^{-1}$, es decir, $xz = yx$. Así, $\forall x \in G$, $y * xH = (yx) * H = (xz) * H = xzH = xH$. De donde, al ser la acutación efectiva, se tiene que $y = e$.

[$\Leftarrow$] Definimos $*G \times (G/H)_i \rightarrow (G/H)_i$ tal que $x * yH := xyH$. Veamos que se trata de una actuación:

Si $x, y, z \in G$

$$x * (y * zH) = x * (yzH) = xyzH = (xy)zH = (xy) * zH$$
$$e * xH = exH = xH.$$

Veamos finalmente que $*$ es efectiva: Sea $x \in G$ tal que $\forall y \in G$, $x * yH = yH$. Entonces

$$y^{-1}H = x * y^{-1}H = xy^{-1}H \ \rightarrow \ yxy^{-1} \in H \ \rightarrow \ x \in y^{-1}Hy = H^y \ \Rightarrow \ x \in \cap_{y \in G} H^y = \{e\},$$

es decir, $x = e$. $\clubsuit$

Ex. 90 *Sea X un conjunto finito. Demostrar que el grupo $S(X)$ de todas las biyecciones de X en sí mismo, con la operación de composición $\circ$, es el mayor grupo efectivo de transformaciones sobre X.*

$\equiv$

Primero veamos que $S(X)$ actúa efectivamente sobre X: Definimos $* : S(X) \times X \rightarrow X$ tal que, si $f \in S(X)$, $x \in X$, $f * x := f(x)$.

$$\forall f, g \in S(X), \forall x \in X, f * (g * x) = f * g(x) = f(g(x)) = (f \circ g)(x)$$
$$Id_X * x = Id_X(x) = x$$
$$Si, \ \forall x \in X, \ \ f * x = x \ \rightarrow \ \forall x \in X, \ \ f(x) = x \ \rightarrow f = Id_X.$$

Decir que $S(X)$ es el mayor grupo que actúa efectivamente sobre X significa que, si G es un grupo que actúa efectivamente sobre X mediante la actuación $\bullet : G \times X \to X$, entonces existe un *monomorfismo* de grupos (homomorfismo inyectivo) de G en $S(X)$. Veámoslo

Para ello definimos la aplicación $\varphi : G \to S(X)$ tal que, si $g \in G$, entonces $\varphi(g)$ es tal que, $\forall x \in X$, $\varphi(g)(x) := g * x$.

φ bien definida: Si $g \in G$, hay que ver que $\varphi(g) \in S(G)$, es decir, que $\varphi(g)$ es una biyección de X en X. Para cada $x \in X$, es evidente que $\varphi(g)(x) = g * x \in X$. Si $x, y \in X$ son tales que $\varphi(g)(x) = \varphi(g)(y)$, entonces

$$\varphi(g)(x) = \varphi(g)(y) \ \to \ g * x = g * y \ \to \ x = e * x = (g^{-1}g) * x = g^{-1} * (g * x)$$

$$= g^{-1} * (g * y) = (g^{-1}g) * y = e * y = y.$$

Al ser X un conjunto finito, toda aplicación inyectiva de X en sí mismo es biyectiva, luego $\varphi(g)$ es biyectiva.

φ homomorfismo: Si $g, h \in G$, $\forall x \in X$,

$$\varphi(gh)(x) = (gh) * x = g * (h * x) = g * (\varphi(h)(x)) = \varphi(g)(\varphi(h)(x))$$

$$= (\varphi(g) \circ \varphi(h))(x) \Rightarrow \ \varphi(gh) = \varphi(g) \circ \varphi(h).$$

φ inyectiva: Si $g \in Ker\ \varphi$, como $\varphi(g) = Id_X$, se tiene

$$\forall x \in X, \ \varphi(g)(x) = x \ \to \ \forall x \in X, \ g * x = x \ \overset{* \ efectiva}{\to} \ g = e. \ \clubsuit$$

Ex. 91 *Sea G un grupo y H un subgrupo de G. Demostrar que H actúa sobre G mediante: $\forall h \in H$, $\forall g \in G$, $h * g := hg$. Dado un elemento $g \in G$, hallar la órbita de g y el estabilizador de g.*

$\equiv$

Veamos primero $*$ es una actuación de H sobre G: Dados $h_1, h_2 \in H$, $g \in G$,

$h_1 * (h_2 * g) = h_1(h_2 g) = (h_1 h_2)g$
$e * g = eg = g$
Si $h \in H$ es tal que, $\forall g \in G$, $h * g = g \ \to \ \forall g \in G$, $hg = g \ \overset{para\ g=h}{\longrightarrow} \ hh = h \ \to \ h = e$

$\Rightarrow$ $*$ *es una actuación efectiva.*

Recordemos que, dado $g \in G$, la órbita de g es el conjunto $H * g = \{h * g : \ h \in H\}$ y el estabilizador de g es el conjunto $est(g) = \{h \in H : \ h * g = g\}$. Por tanto

$$H * g = Hg \ (\textit{el cogrupo a la derecha de } g)$$
$$est(g) = \{h \in H : \ h * g = g\} = \{h \in H : \ hg = g\} = \{e\}. \ \clubsuit$$

Ex. 92 *Sea G un grupo que actúa sobre X. Demostrar que si dos elementos de X están en la misma órbita, entonces sus estabilizadores son subgrupos conjugados de G.*

$\equiv$

Sean $x, y \in X$ tales que pertenecen a una misma órbita, es decir, $\exists z \in X$ tal que $x, y \in G * z$ (donde $*$ es la actuación de G sobre X). Entonces: $\exists g, h \in G$ tales que

$$\left.\begin{array}{l} x = g*z \ \rightarrow \ g^{-1}*x = z \\ y = h*z \end{array}\right\} \Rightarrow y = h*z = h*(g^{-1}*x) = (hg^{-1})*x \overset{\text{llamando } u:=hg^{-1}\in G}{=} u*x.$$

Para ver que los estabilizadores de x y de y son subgrupos conjugados, hay que verificar que $\exists v \in G$ de modo que $est(y) = v^{-1}[est(x)]v$. Así pues todo se reduce a demostrar que $est(y) = u[est(x)]u^{-1}$, siendo $u \in G$ el elemento de G anterior.
[$\subseteq$] Si $w \in est(y)$, entonces, como $w * y = y$,

$$(u^{-1}wu)*x = (u^{-1}w)*(u*x) = (u^{-1}w)*y = u^{-1}*(w*y) = u^{-1}*y = x \ \Rightarrow \ u^{-1}wu \in est(x).$$

Por tanto, $w \in u[est(x)]u^{-1}$.
[$\supseteq$] Si $w \in u[est(x)]u^{-1}$, entonces $\exists v \in est(x)$ tal que $w = uvu^{-1}$. Así

$$w*y = (uvu^{-1})*y = (uv)*(u^{-1}*y) = (uv)*x = u*(v*x) = u*x = y \ \Rightarrow \ w \in est(y). \ \clubsuit$$

Ex. 93 *Sean H, K subgrupos de G. Sabemos que K actúa sobre $(G/H)_i$ por $x*(yH) = xyH$. Hallar el estabilizador de une elemento de $(G/H)_i$ y también el número de elementos de su órbita.*

$\equiv$

Fijado un elemento $xH \in (G/H)_i$, sabemos que

$$est(xH) = \{\, y \in K \ : \ y*(xH) = xH\} = \{y \in K : \ yxH = xH\} = \{y \in K : \ x^{-1}yx \in H\}$$

$$= \{y \in K : \ y \in xHx^{-1}\} = K \cap (xHx^{-1}).$$

El número de elementos de $K*(xH)$ coincide con el índice del subgrupo $K \cap (xHx^{-1})$ respecto de K, es decir, con $[K : K \cap (xHx^{-1})]$. $\clubsuit$

1.6. Grupos simples

Ex. 94 *Sea G un grupo de orden $p \cdot q$, con $p < q$ números primos.*
1) Demostrar que G es cíclico cuando $q \not\equiv 1 \ (mod.\ p)$.
2) Qué puede decirse de G cuando $q \equiv 1 \ (mod.\ p)$?

$\equiv$

Antes de meternos a resolver este problema, creemos que es conveniente hablar algo acerca de los *Teoremas de Sylow*.

Teorema 1 *[Primer teorema de Sylow, 1872] (T1S)*
Sea G un grupo finito y sea p un número primo. Si p^k es un divisor de $o(G)$, entonces G admite algún subgrupo de orden p^k.

Definición 1 *[Subgrupo p-Sylow]*

Sea p un divisor primo del orden del grupo finito G. Supongamos que la potencia p^k divide a $o(G)$, pero no así p^{k+1}. Entonces, a cualquier subgrupo de orden p^k (de existencia garantizada por $T1S$) se le denomina subgrupo p-Sylow.

Teorema 2 *[Segundo teorema de Sylow] ($T2S$)*

Si H y K son dos subgrupos p-Sylow de G, entonces existe $x \in G$ tal que $H = x^{-1}Kx$, es decir, H y K son conjugados..

Teorema 3 *[Tercer teorema de Sylow] ($T3S$)*

Sea G un grupo finito. Si indicamos por n_p el número de p-subgrupos de Sylow que tiene G, entonces:

(i) n_p *divide a* $o(G)$

(ii) $n_p \equiv 1 \ (mod.\ p)$

(iii) Si H es un subgrupo p-Sylow cualquiera, entonces $n_p = [G : N(H)]$.

Volvamos al ejercicio.

1) Supongamos que $q \not\equiv 1 \ (mod.\ p)$. Sean n_p y n_q los números de subgrupos p-Sylow y q-Sylow, respectivamente. Del $T3S$, $n_p \equiv 1 \ (mod.\ p)$, por tanto n_p y p son primos entre sí. Del mismo teorema, n_p divide a $o(G) = pq$ y, como $mcd(p, n_p) = 1$, se tiene que $n_p \mid q$. Pero, al ser q primo, $n_p \in \{1, q\}$, de donde, como $q \not\equiv 1 \ (mod.\ p)$, se deduce que $n_p = 1$. Razonando de manera análoga se obtiene que $n_q = 1$. Consecuentemente, al haber sólo un subgrupo p-Sylow, llamémosle H_1, se tiene que $o(H_1) = p$; similarmente, si H_2 es el único subgrupo q-Sylow, entonces $o(H_2) = q$. Por tanto, al tratarse de grupos de orden primo, son cíclicos. Así pues, supongamos que $H_1 = \langle\ x_1\ \rangle$ y $H_2 = \langle\ x_2\ \rangle$. Consideremos el subgrupo de G generado por el elemento x_1x_2, es decir, $H = \langle\ x_1x_2\ \rangle$. Todo se reduce a probar que $H = G$.

Al ser H subgrupo de G, se tiene que $o(H)$ es un divisor de $o(G) = pq$, es decir, $o(H) \in \{1, p, q, pq\}$. Como además $x_1x_2 \neq e$, de lo contrario $H_1 = H_2$ lo que es absurdo pues $p \neq q$, tenemos que $o(H) \neq 1$ y nos planteamos tres posibilidades:

Una. $o(H) = p$. Entonces $H = H_1$ y

$$x_1x_2 \in H_1 = \langle\ x_1\ \rangle \ \rightarrow\ x_2 \in H_1,\ \textit{Absurdo.}$$

Dos. $o(H) = q$. Entonces $H = H_2$ y

$$x_1x_2 \in H_2 = \langle\ x_2\ \rangle \ \rightarrow\ x_1 \in H_2,\ \textit{Absurdo.}$$

Tres. $o(H) = pq$. Ahora hemos terminado ya que $H = G$.

2) Suponiendo ahora que $q \equiv 1 \ (mod.\ p)$, de nuevo haciendo uso de $T3S$, como $n_p \mid o(G) = pq$, $mcd(n_p, p) = 1$, se plantean dos posibilidades:

Una. $n_p = 1$. Entonces, de nuevo $T3S$ nos dice que $n_q \mid pq$, $mcd(n_q, q) = 1$, por lo que $n_q \mid p$; pero, si $n_q = p$ ello nos lleva a que $p = n_q \equiv 1 \ (mod.\ q)$ y así $q \mid p - 1 < q - 1$, absurdo. Por tanto, $n_q = 1$ y de lo hecho en el primer apartado obtenemos que G es cíclico.

Dos. $n_p = q$. Ahora lo único que podemos afirmar es que G admite q subgrupos p-Sylow conjugados entre sí. Conviene observar que, en general, si estamos en esta posibilidad, es decir, con que $n_p = q \equiv 1\ (mod.\ p)$, G no tiene porqué ser cíclico, ni tan siquiera abeliano, como prueba el siguiente ejemplo:

Considérese $G := \Sigma_3$ (el grupo simétrico de las permutaciones de tres elementos). Claramente, $o(G) = o(\Sigma_3) = 3! = 6 = 2 \cdot 3$. Es decir, $p = 2$, $q = 3$. Estamos en la situación del segundo apartado anterior, ya que $q = 3 \equiv 1\ (mod.\ 2 = p)$, y Σ_3 no es abeliano aunque admite $n_p = q = 3$ subgrupos $p = 2$-Sylow conjugados entre sí: $\{e, (12)\}$, $\{e, (13)\}$, $\{e, (23)\}$. ♣

Ex. 95 *Demostrar que un grupo de orden $2p$, con p primo, o es cíclico o es isomorfo al grupo dihédrico D_p.*

≡

Sea G un grupo tal que $o(G) = 2p$, con p primo. Antes de ponernos a resolver el problema, observemos que podemos suponer que $p > 2$, de lo contrario, si $p = 2$ se tendría que $o(G) = 4$ y entonces se cumpliría la tesis del enunciado, ya que de un ejercicio resuelto anteriormente sabemos que G es isomorfo a $\mathbf{Z}_4$, que es cíclico, o es isomorfo al Vieregruppe de Klein, que a su vez es isomorfo al dihédrico D_2.

De $T1S$, sabemos que G tiene subgrupos 2-Sylow, sea n_2 la cantidad de dichos subgrupos. Del $T3S$, $n_2 \mid 2p$, $mcd(n_2, 2) = 1$, por lo que $n_2 \mid p$, es decir, $n_2 \in \{1, p\}$. Tenemos pues dos posibilidades:

Una. $n_2 = 1$. En este caso, si n_p indica la cantidad de subgrupos p-Sylow de G, tenemos que $n_p \mid 2p$, $mcd(n_p, p) = 1$, de lo que $n_p \mid 2$, es decir, $n_p \in \{1, 2\}$, pero $n_p \equiv 1\ (mod.\ p)$ implica que $n_p \neq 2$ y tenemos que $n_p = 1$. Entonces estamos en la misma situación del primer apartado del ejercicio anterior, es decir, $o(G) = 2p$, con un único subgrupo 2-Sylow, $H_1 := \langle\ x_1\ \rangle$, y un único subgrupo p-Siylow, $H_2 := \langle x_2\ \rangle$. Por tanto, $o(H_1) = 2$, $o(H_2) = p$. Como antes, considerando el subgrupo $H := \langle x_1 x_2\ \rangle$, todo se reduce a ver que $H = G$, por lo que G será, en este caso, cíclico: Como $o(x_1x_2) \in \{1, 2, p, 2p\}$, distinguimos los casos siguientes

Uno. $o(x_1x_2) = 1$. Entonces $x_1x_2 = e$, lo que implica que $x_2 = x_1^{-1} \in H_1$, absurdo, ya que $o(x_2) = o(H_2) = p > 2 = o(H_1)$.

Dos. $o(x_1x_2) = 2$. Ahora, como sólo hay un subgrupo 2-Sylow, sólo hay un subgrupo de orden 2, por lo que $H_1 = \langle\ x_1x_2\ \rangle$, de donde de nuevo $x_2 \in H_1$, que es absurdo.

Tres. $o(x_1x_2) = p$. Como antes, $\langle\ x_1x_2\ \rangle = H_2$, de lo que $x_1 \in H_2$, absurdo, pues $o(x_1) = 2 \not\mid p = o(H_2)$.

Cuatro. $o(x_1x_2) = 2p$. Claramente, $G = \langle\ x_1x_2\ \rangle = H$, como queríamos.

Dos. $n_2 = p$. En este caso, de lo visto en la primera posibilidad, $n_p = 1$, es decir hay solamente un subgrupo p-Sylow que, al tener orden primo, es cíclico y tiene la forma $H = \langle\ x\ \rangle = \{e, x, x^2, ..., x^{p-1}\}$. Sean $H_1 = \{e, y_1\}$, $H_2 = \{e, y_2\}$, ..., $H_p = \{e, y_p\}$, los p subgrupos 2-Sylow que tiene G. Obviamente, $G = H \cup H_1 \cup H_2 \cup ... \cup H_p = H \cup$

$\{y_1, y_2, ..., y_p\}$. Vamos a hallar los elementos $y_2, y_3, ..., y_p$ en función de x, y_1

$$xy_1 \notin H \cup H_1 \ \rightarrow \ xy_1 \in H_2 \cup H_3 \cup ... \cup H_p \ \overset{sup.que}{\rightarrow} \ xy_1 \in H_2 \rightarrow \ xy_1 = y_2$$
$$xy_2 \notin H \cup H_1 \cup H_2 \ \rightarrow \ xy_2 \in H_3 \cup H_4 \cup ... \cup H_p \ \overset{sup.que}{\rightarrow} \ xy_2 \in H_3 \rightarrow \ xy_2 = x^2 y_1 = y_3$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$xy_{p-1} \notin H \cup H_1 \cup ... \cup H_{p-1} \ \rightarrow \ xy_{p-1} \in H_p \ \rightarrow \ xy_{p-1} = x^{p-1} y_1 = y_p$$

$$\Rightarrow \ G = \{e, x, x^2, ..., x^{p-1}, y_1, xy_1, x^2 y_1, ..., x^{p-1} y_1\} \ \simeq \ D_p \ . \ \clubsuit$$

Ex. 96 *Sea G un grupo finito con un subgrupo normal H de orden p^k, con p primo y $k > 0$. Demostrar que H está contenido en todo subgrupo p-Sylow de G.*

$\equiv$

Sea F un subgrupo p-Sylow de G. Entonces, existen n, m enteros positivos tales que $n \geq k$, $o(G) = p^n m$, $p \not| m$. Al tratarse de un subgrupo normal, claramente $FH = HF$, por lo que HF es un subgrupo de G y además $o(HF) = \frac{o(H)o(F)}{o(H \cap F)}$. Por tanto, como $o(H \cap F) \mid o(H)$, existe un entero r tal que $0 \leq r \leq k$, $o(H \cap F) = p^r$. Así, $o(HF) = p^{k+n-r}$. Como $F \subseteq HF$, se tiene

$$p^n \ = \ o(F) \ \leq \ o(HF) \ = \ p^{k+n-r} \ \Rightarrow \ k - r \geq 0 \ \Rightarrow \ k - r = 0,$$

ya que $o(HF) \mid o(G) = p^n m \ \rightarrow \ p^{k+n-r} \mid p^n m$. Consecuentemente, como $k = r$, tenemos que $o(H) = o(H \cap F)$, de donde $H = H \cap F$, i.e., $H \subseteq F$. $\clubsuit$

Ex. 97 *Sea H un subgrupo normal de índice finito de un grupo G. Demostrar que si $p^k | \ [G : H]$, con p primo, $k > 0$, entonces G contiene un subgrupo K tal que $[K : H] = p^k$.*

$\equiv$

Al ser H normal, G/H es un grupo de orden $[G : H]$. Como p^k es un divisor de $o(G/H)$, del $T1S$ sabemos que existe un subgrupo $\widehat{K}$ de G/H tal que $o(\widehat{K}) = p^k$. Consideramos

$$K \ := \ \{ \ x \in G \ : \ xH \in \widehat{K} \}.$$

K es un subgrupo de G: Si $x, y \in K$, como $xH, yH \in \widehat{K}$, se tiene que $xy^{-1}H = (xH)(yH)^{-1} \in \widehat{K}$, i.e., $xy^{-1} \in K$.

Por tanto, como $H \subseteq K$, H es un subgrupo normal de K y $\widehat{K} = K/H$. Así

$$[K : H] \ = \ o(K/H) \ = \ o(\widehat{K}) \ = \ p^k. \ \clubsuit$$

Ex. 98 *Un grupo G se dice que es simple siempre que no admite subgrupos propios normales. Demostrar que un grupo de orden 30 nunca es simple.*

$\equiv$

Sea G un grupo tal que $o(G) = 30 = 2 \cdot 3 \cdot 5$. Sean n_2, n_3, n_5 los números de subgrupos 2, 3 y 5-Sylow, respectivamente. Del $T3S$

$$\begin{array}{l} n_2 | \ 15, \ n_2 \equiv 1 \ (mod,2) \ \rightarrow \ n_2 \in \{1,3,5,15\} \\ n_3 | \ 10, \ n_3 \equiv 1 \ (mod,3) \ \rightarrow \ n_3 \in \{1,10\} \\ n_5 | \ 6, \ n_3 \equiv 1 \ (mod,5) \ \rightarrow \ n_5 \in \{1,6\}. \end{array}$$

Consideramos dos posibilidades:

Una. $n_3 = 1$, ó, $n_5 = 1$. Entonces, si $n_3 = 1$, sólo hay un subgrupo 3-Sylow, por lo que todos sus conjugados coinciden con él, es decir, se trata de un subgrupo normal y no propio; si $n_5 = 1$, habría análogamente un único subgrupo 5-Sylow que sería normal y propio.

Dos. $n_3 \neq 1$ y $n_5 \neq 1$. Ahora, $n_3 = 10$ y $n_5 = 6$. Así, sean

$$H_1, H_2, ..., H_{10} \ \text{ y } \ \mathrm{K_1, k_2, ..., K_6}$$

los subgrupos 3-Sylow y 5-Sylow de G, respectivamente. Para cada $1 \leq i \neq j \leq 10$, como $o(H_i \cap H_j) \mid 3$, se tiene que $H_i \cap H_j = \{e\}$. Similarmente, para $1 \leq i \neq j \leq 6$, $K_i \cap K_j = \{e\}$. Además, para $1 \leq i \leq 10$, $1 \leq j \leq 6$, también $H_i \cap K_j = \{e\}$, ya que su orden debe dividir a 3 y a 5. Consecuentemente

$$card(H_1 \cup H_2 \cup ... \cup H_{10} \cup K_1 \cup K_2 \cup ... \cup K_6) \ = \ 10 \cdot 2 \ + \ 6 \cdot 4 \ + \ 1 \ = \ 45,$$

lo que es absurdo, pues G sólo tiene 30 elementos. ♣

Nota 7 Observar que en realidad lo que hemos demostrado es que todo grupo de orden 30 posee un subgrupo normal de orden 3 o de orden 5.

Ex. 99 *Demostrar que todo grupo de orden p^2q, con $p \neq q$ primos, nunca es simple.*

≡

Sea G un grupo de orden p^2q. Sean n_p y n_q los números de subgrupos p-Sylow y q-Sylow, respectivamente, que tiene G. Consideramos dos posibilidades:

Una. $p > q$. Como $n_p | q$, $n_p \equiv 1 \ \ (mod.p)$, tenemos que $n_p = 1$. Por tanto, sólo hay un subgrupo p-Sylow y, al coincidir con todos sus conjugados (ya que éstos también son subgrupos p-Sylow), se trata de un subgrupo normal.

Dos. $p < q$. Ahora, tenemos que $n_p \in \{1, q\}$, $n_q \in \{1, p, p^2\}$, $n_q \equiv 1 \ \ (mod.q)$. Así, $n_q \in \{1, p^2\}$. Consideramos pues dos alternativas:

a) $n_p = 1$ ó $n_q = 1$. Entonces hay garantizada la existencia de un subgrupo normal, de orden p^2 si $n_p = 1$, o de orden q si $n_q = 1$.

b) $n_p \neq 1$, $n_q \neq 1$. Ahora, $n_p = q$ y $n_q = p^2$. Sea H un subgrupo p-Sylow. Sean

$$K_1, K_2, ..., K_{p^2}$$

los subgrupos q-Sylow. Dados $1 \leq i \neq j \leq p^2$, tenemos

$$\left.\begin{array}{l} o(K_i \cap K_j) \mid q \ \rightarrow \ K_i \cap K_j = \{e\} \\ o(H \cap K_i) \mid q \ \rightarrow \ H \cap K_i = \{e\} \end{array}\right\}$$

$$\Rightarrow \ card(H \cup K_1 \cup ... \cup K_{p^2}) = 1 + 1 \cdot (p^2 - 1) + p^2(q-1) = p^2 q.$$

Ello supone una contradicción, ya que entonces $G = H \cup K_1 \cup ... \cup K_{p^2}$, pero, como $n_p = q > 1$, sabemos que existe otro subgrupo p-Sylow H' distinto de H; si $x \in H' \setminus H$, como $H' \cap K_i = \{e\}$, $1 \leq i \leq p^2$, se tiene que $x \notin H \cup K_1 \cup ... \cup K_{p^2}$. ♣

Ex. 100 *[Criterios de no-simplicidad]*
1.- Sea G un grupo tal que $o(G)$ no es primo y admite un divisor primo p de forma que $o(G)$ no tiene divisores propios congruentes con 1 $(mod.p)$. Entonces G no es simple.
2.- Si $o(G) = pq^k$, $p < q$ primos, entonces G no es simple.
3.- Sea H un subgrupo propio de G tal que $o(G) \not| \ ([G:H])!$. Entonces H contiene un subgrupo propio normal de G.

≡
1) Distinguimos dos casos:
Primer caso: $o(G) = p^k$. Entonces, al tratarse de un grupo con orden potencia de primo, es bien sabido que G admite algún subgrupo propio normal (explícitamente, dicho subgrupo es el centro de G en el caso de que G no sea abeliano, o algún subgrupo cíclico si G es abeliano).
Segundo caso: $o(G) = p^k m$, $p \not| \ m$. Del T3S sabemos que, si n_p es el número de subgrupos p-Sylow de G, entonces $n_p | m$, $n_p \equiv 1 \ (mod.p)$. Por hipótesis $n_p = 1$, por tanto sólo hay un subgrupo p-Sylow, por lo que, al coincidir con sus conjugados, es normal, y obviamente propio pues su orden es $p^k < o(G)$.
2) Como $o(G) = pq^k$, $p < q$ primos, se tiene que $o(G)$ no tiene divisores propios congruentes con 1 $(mod.q)$. Podemos entonces aplicar el criterio anterior.
3) Sea $\Sigma(G/H)$ el grupo de las permutaciones de G/H (biyecciones de G/H en sí mismo). Definimos

$$\begin{array}{rcl} f & : & G \longrightarrow \Sigma(G/H) \\ & & x \ \rightarrow \ f(x)(yH) = xyH, \quad yH \in G/H. \end{array}$$

Veamos que f es un homomorfiso de grupos: Si $x, y \in G$, entonces, dada $zH \in G/H$,

$$f(xy)(zH) = (xy)zH = x(yzH) = f(x)(yzH) = f(x)[f(y)(zH)] = [f(x) \circ f(y)](zH),$$

es decir, $f(xy) = f(x) \circ f(y)$. Además, el núcleo del homomorfismo f es un subgrupo de H ya que

$$x \in Ker \ f \ \Rightarrow \ f(x) = Id_{G/H} \ \Rightarrow \ f(x)(H) = H \ \Rightarrow \ xH = H \ \Rightarrow \ x \in H.$$

Así

$$G/Ker \ f \cong f(G) \ \Rightarrow \ [G : Ker \ f] = o(G/Ker \ f) = o(f(G)) \mid o(\Sigma(G/H)) = ([G:H])!$$

Como, por hipótesis, $o(G)$ no divide a $([G:H])!$, queda claro que $o(Ker \ f) > 1$, con lo que tenemos un subgrupo $Ker \ f$ que es normal y propio. ♣

Ex. 101 *Demostrar que todo grupo simple de orden menor que 60 tiene orden primo.*

$\equiv$

Sea G un grupo simple tal que $o(G) < 60$. Suponiendo que $o(G)$ no es primo, consideramos las siguientes posibilidades:

Una. $o(G)$ es potencia de primo. Entonces

$$o(G) \in \{4,\ 8,\ 9,\ 16,\ 25,\ 27,\ 32,\ 49\}.$$

Del Criterio 1 (primer caso) sabemos que G no es simple, es decir, esta posibilidad no se puede dar.

Dos. $o(G)$ es de la forma $o(G) = pq^k$, $p < q$ primos. Ahora

$$o(G) \in \{6,\ 10,\ 14,\ 15,\ 18,\ 21,\ 22,\ 26,\ 33,\ 34,\ 35,\ 38,\ 39,\ 46,\ 50,\ 51,\ 54,\ 55,\ 57,\ 58\}.$$

Del Criterio 2 sabemos que G no es simple, luego esta posibilidad tampoco se puede dar.

Tres. $o(G)$ es de la forma $o(G) = p^2q$, $p \neq q$ primos. Aquí

$$o(G) \in \{12,\ 20,\ 28,\ 44,\ 45,\ 52\}.$$

Del Ejercicio 98 sabemos que G no es simple.

Cuatro. $o(G) \in \{24,\ 30,\ 36,\ 40,\ 42,\ 48,\ 56\}$. Dentro de esta posibilidad distinguimos

a) $o(G) = 30$. Aplicar el Ejercicio 98.

b) $o(G) \in \{40,\ 42\}$. Aquí basta con aplicar el Criterio 1, ya que $40 = 2^3 \cdot 5$ no tiene divisores propios congruentes con 1 $(mod.\ 5)$, y $42 = 2 \cdot 3 \cdot 7$ no tiene divisores propios congruentes con 1 $(mod.\ 7)$.

c) $o(G) \in \{24,\ 36,\ 48\}$. Ahora aplicamos el Criterio 3 del siguiente modo

$$Si\ \ o(G) = 24 = 2^3 \cdot 3,\ tomar\ H\ con\ o(H) = 8\ \rightarrow \begin{cases} [G:H] = 3 \\ o(G) = 24 \not| 3! = ([G:H])! \end{cases}$$

$$Si\ \ o(G) = 36 = 2^2 \cdot 3^2,\ tomar\ H\ con\ o(H) = 9\ \rightarrow \begin{cases} [G:H] = 4 \\ o(G) = 36 \not| 4! = ([G:H])! \end{cases}$$

$$Si\ \ o(G) = 48 = 2^4 \cdot 3,\ tomar\ H\ con\ o(H) = 16\ \rightarrow \begin{cases} [G:H] = 3 \\ o(G) = 48 \not| 3! = (G:H])! \end{cases}$$

d) $o(G) = 56$. Haciendo unas pocas cuentas se observa que éste es el único caso que nos queda. Como $o(g) = 56 = 2^3 \cdot 7$, sean n_2 y n_7 los números de subgrupos 2-Sylow y 7-Sylow, respecitvamente. Del T3S sabemos que $n_2 \in \{1,7\}$, $n_7 \in \{1,8\}$. Si $n_2 = 1$, ó, $n_7 = 1$ todo claro, como hemos explicado varias veces antes (un único subgrupo p-Sylow es siempre normal y propio). Suponiendo que que $n_2 = 7$ y $n_7 = 8$, se tiene que, considerando H, H' dos de los 7 subgrupos 2-Sylow y $K_1, K_2, ..., K_8$ los distintos subgrupos 7-Sylow de G, entonces, ya que las intersecciones $(H \cup H') \cap (K_1 \cup K_2 \cup ... \cup K_8)$ y $K_i \cap K_j$, $1 \leq i \neq j \leq 8$, se reducen al neutro,

$$card(H \cup H' \cup K_1 \cup ... \cup K_8) = card(H \cup H') + card(K_1 \cup K_2 \cup ... \cup K_8) - 1$$

$$= card(H) + card(H') - card(H \cap H') + 8 \cdot (7-1) + 1 - 1 \geq 8 + 8 - 4 + 48 = 60,$$

lo que es absurdo, ya que $o(G) < 60$. ♣

Nota 8 Curioso e interesante es resaltar la gran escasez de grupos simples, no abelianos por supuesto (éstos son los $\mathbf{Z}_p$, con p primo). De hecho, los únicos grupos simples no abelianos de orden menor que 1000 son los siguientes: de orden 60 (el famoso grupo A_5 de las permutaciones pares de 5 elementos) y los de orden 168, 320, 504, 660. El problema de determinar qué grupos finitos son simples (*Clasificación de los grupos simples*) ha tenido una feliz conclusión hace relativamente poco:

–A principio de los años 60 aparece el Teorema de Feit-Thompson (255 páginas) que establece que un grupo simple no abeliano ha de tener orden par.

–En1972, Daniel Gorenstein elabora un plan para completar la clasificación de los grupos simples.

–En 1976, M. Aschbacher, empleando métodos de Thompson, junto con los geométricos de B. Fischer, consigue desarrollar técnicas que se manifiestan suficientes para obtener la clasificación.

–En 1980, R. L. Griess anuncia que ha construido el "Mosntruo"(nombre, debido a J. H. Conway, con el que se conoce al mayor de los grupos simples *esporádicos*), el orden es en efecto monstruoso:

$$808,017_8424,794_7512,875_6886,459_5904,961_4710,757_3005,754_2368,000_1000,000.$$

i.e. ochocientos ocho mil diecisiete octillones...

Se trata de un grupo de rotaciones en 196,883 dimensiones.

–En 1981, D. Gorenstein declara, en representación del equipo, que todos los grupos simples finitos han sido clasificados. La demostración tiene más de 10,000 páginas. Ahora hace falta simplificarla y hacerla comprensible!!

Ex. 102 *Sea G un grupo finito que contiene exactamente un subgrupo p-Sylow para cada primo p divisor de $o(G)$. Demostrar que G es isomorfo al producto directo de todos sus subgrupos de Sylow.*

≡

Sea

$$o(G) \;=\; p_1^{k_1} \cdot p_2^{k_2} \cdot ... p_m^{k_m}, \quad p_i \text{ primo}, \quad k_i \in \mathbf{N}, \quad 1 \leq i \leq m.$$

Para cada $i = 1, 2, ..., m$, sea H_i el único subgrupo p_i-Sylow que tiene G. Definimos

$$\begin{array}{rcl} f & : & H_1 \times H_2 \times ... \times H_m \longrightarrow G \\ & & (x_1, x_2, ..., x_m) \;\rightarrow\; f(x_1, x_2, ..., x_m) = x_1 x_2 ... x_m. \end{array}$$

Claramente, f es una aplicación bien definida. Verificamos las siguientes propiedades de f:

f homomorfismo: Observemos antes que, al ser subgrupos p-Sylow únicos, los $H_1, H_2, ..., H_m$ son subgrupos normales, por lo que se tiene que, si $x_i \in H_i$, $x_j \in H_j$, $i \neq j$, entonces $x_i x_j = x_j x_i$:

$$\left.\begin{array}{l} x_i x_j x_i^{-1} x_j^{-1} = x_i (x_j x_i^{-1} x_j^{-1}) \in x_i (x_j H_i x_j^{-1}) = x_i H_i = H_i \\ x_i x_j x_i^{-1} x_j^{-1} = (x_i x_j x_i^{-1}) x_j^{-1} \in (x_i H_j x_i^{-1}) x_j^{-1} = H_j x_j^{-1} = H_j \end{array}\right\}$$

$$\Rightarrow\ x_i x_j x_i^{-1} x_j^{-1} \in H_i \cap H_j = \{e\}$$
$$\Rightarrow\ x_i x_j x_i^{-1} x_j^{-1} = e\ \Rightarrow\ x_i x_j = x_j x_i.$$

Así

$$f((x_1, x_2, ..., x_m)(y_1, y_2, ..., y_m)) = f(x_1 y_1, x_2 y_2, ..., x_m y_m) = x_1 y_1 x_2 y_2 ... x_m y_m$$
$$= x_1 x_2 ... x_m y_1 y_2 ... y_m = f(x_1, x_2, ..., x_m) f(y_1, y_2, ..., y_m).$$

f inyectivo: Si $(x_1, x_2, ..., x_m) \in Ker\ f$, entonces $x_1 x_2 ... x_m = e$. Al tratarse de subgrupos normales se ve fácilmente que todos los productos de estos subgrupos son subgrupos cuyo orden es el producto de los órdenes de sus factores, así

$$x_2 x_3 ... x_m = x_1^{-1} \Rightarrow x_1 \in H_1 \cap H_2 H_3 ... h_m \Rightarrow x_1 = e = x_2 x_3 ... x_m.$$

De manera análoga, a partir de que $x_2 x_3 ... x_m = e$ se ve que $x_2 = e$, y así hasta llegar a que

$$x_1 = x_2 = ... = x_m = e.$$

f sobre: Dado $x \in G$, como

$$o(H_1 H_2 ... H_m) = p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_m^{k_m} = o(G) \Rightarrow G = H_1 H_2 ... H_m,$$

de lo que $x \in H_1 H_2 ... H_m$, es decir, $\exists x_1 \in H_1$, $\exists x_2 \in H_2$,...,$\exists x_m \in H_m$ tales que
$$x = x_1 x_2 ... x_m = f(x_1, x_2, ..., x_m). \clubsuit$$

Ex. 103 *Sea p primo tal que p^k divide al orden del grupo finito G. Demostrar que el número de subgrupos de orden p^k de G es congruente con 1 (mod. p). (Resultado de G. Fröbenius)*

≡

La resolución que damos de este ejercicio es una adaptación de la demostración del mismo que aparece en el texto [3, pág. 39-42].

Sea $o(G) = p^n m$, $p \not| m$, $n > k$ (ya que si $n = k$ el resultado es consecuencia del T3S, ya que los subgrupos de orden p^n son subgrupos p-Sylow). Consideramos la familia de partes de G

$$\mathcal{F} := \{ S \subseteq G\ \ card(S) = p^k \},$$

Es decir, $\mathcal{F}$ es la colección de todos los subconjuntos de G que tienen exactamnete p^k elementos. Obsérvese que G actúa sobre $\mathcal{F}$ mediante $S \rightarrow x * S = xS$. Explícitamente

$$* : G \times \mathcal{F} \longrightarrow \mathcal{F}$$
$$(x, S) \rightarrow x * S = xS$$

es una aplicación bien definida que cumple las condiciones de ser una *actuación de un grupo sobre un conjunto*. Consecuentemente, en $\mathcal{F}$ la relación

$$S \sim S' \leftrightarrow \exists\ x \in G \text{ tal que } x * S = S',$$

es de equivalencia. Por tanto, existen h clases de equivalencia

$$G * S_1,\ G * S_2,\ ...,\ G * S_h$$

tales que el conjunto cociente $\mathcal{F}/\sim = \{G * S_1, G * S_2, ..., G * S_h\}$. Entonces

$$\mathcal{F} = G * S_1 \cup G * S_2 \cup ... \cup G * S_h.$$

De la Combinatoria finita sabemos que

$$card(\mathcal{F}) = \left(\begin{array}{c} p^n m \\ p^k \end{array} \right) = \frac{p^n m(p^n m - 1)...(p^n m - p^k + 1)}{p^k(p^k - 1)..,2 \cdot 1}$$

$$= p^{n-k}m \cdot (\frac{p^n m - 1}{1})(\frac{p^n m - 2}{2})....(\frac{p^n m - (p^k - 1)}{p^k - 1})$$

$$= p^{n-k}m \cdot (p^n m - 1)(\frac{p^n m}{2} - 1)...(\frac{p^n m}{p^k - 1} - 1)$$

$$= p^{n-k}m \cdot [(-1)^{p^k-1} + v],\ \text{ con } v \in \mathbf{N},\ \ p|\ v.$$

El hecho de que $p|\ v$ se debe a que, como $k < n$, todas las fracciones

$$\frac{p^n m}{2},\ ...,\ \frac{p^n m}{p^k - 1}$$

tienen el factor p en su numerador. Además,como $v \geq p \geq 2$, podemos reescribir

$$card(\mathcal{F}) = p^{n-k}m \cdot [(-1)^{p^k-1} + v] = p^{n-k}m \cdot (1 + pu),\ \text{ con } u \in \mathbf{N}.$$

Para cada $i = 1, 2, ..., h$

$$card(G * S_i)\ |\ o(G) = p^n m \ \Rightarrow\ card(G * S_i) = p^{n_i} m_i,\ \ n_i \leq n,\ m_i \mid m.$$

Supongamos por comodidad que $n_1 = min\{n_1, n_2, ..., n_h\}$. Entonces, al ser $G * S_1, G * S_2, ..., G * S_h$ clases de equivalencia, es decir, conjuntos disjuntos, se tiene que

$$p^{n-k}m \cdot (1 + pu) = card(\mathcal{F}) = \sum_{i=1}^{h} card(G * S_i) = \sum_{i=1}^{h} p^{n_i} m_i = p^{n_1}(m_1 + \sum_{i=2}^{h} p^{n_i - n_1} m_i),$$

de donde

$$p^{n-k-n_1}m(1 + pu) = m_1 + \sum_{i=2}^{h} p^{n_i - n_1} m_i.$$

Ello implica que $n - k - n_1 = 0$, pues $p \not| m_1$. Por tanto, llamando H al estabilizador de S_1, es decir, $H = est(S_1) = \{x \in G :\ xS_1 = S_1\}$, tenemos

$$p^{n-k}m_1 = p^{n_1}m_1 = card(G * S_1) = [G : H].$$

Consecuentemente

$$o(H) \;=\; \frac{o(G)}{[G:H]} \;=\; \frac{p^n m}{p^{n-k}m_1} \;=\; p^k\frac{m}{m_1} \;\geq\; p^k.$$

Por otra parte, tomando $x \in S_1$,

$$Hx \;\subseteq\; S_1 \;\Rightarrow\; o(H) \;=\; card(Hx) \leq\; card(S_1) \;=\; p^k,$$

luego $o(H) = p^k$. Además, $Hx = S_1$, ya que antes vimos que $Hx \subseteq S_1$ y ambos conjuntos tienen el mismo cardinal. Sea $H' := x^{-1}Hx$. Veamos que $G * S_1 = G/H'$:

$$\forall S \in G * S_1 \to \exists y \in G/S = yS_1 = yHx = yx(x^{-1}Hx) = yxH' \in G/H'; G * S_1 \subseteq G/H'$$
$$\forall yH' \in G/H' \to yH' = yx^{-1}Hx = yx^{-1}S_1 = (yx^{-1}) * S_1 \in G * S_1;\; G/H' \subseteq G * S_1.$$

Por tanto, como H' es el único subgrupo perteneciente al conjunto de cogrupos G/H', se tiene que H' es el único subgrupo que pertenece a $G*S_1$, es decir, H' es el único subgrupo de orden p^k contenido en la órbita $G * S_1$. Similarmente, toda órbita $G * S_i$ de cardinal $p^{n-k}m_i$ sólo contiene un único subgrupo de orden p^k. Por tanto, si llamamos r al número de subgrupos de orden p^k de G, está claro que r coincide con el número de órbitas $G * S_i$ de cardinal $p^{n-k}m_i$. Supongamos, también por comodidad, que dichas órbitas son

$$G * S_1,\; G * S_2,\; \ldots\;,\; G * S_r.$$

Para cada $i = 1, 2, ..., r$

$$p^k \;=\; card(S_i) \;=\; \frac{o(G)}{card(G * S_i)} \;=\; \frac{p^n m}{p^{n-k}m_i} \;=\; p^k\frac{m}{m_i}$$

$$\Rightarrow\; m_i = m \;\Rightarrow\; card(G * S_i) = p^{n-k}m.$$

Así, como $\forall i = r+1, r+2, ..., h,\;\; card(G * S_i) = p^{n_i}m_i$, con $n_i > n_1 = n - k$, i.e., $n_i - n + k \geq 1$,

$$p^{n-k}m \cdot (1 + pu) \;=\; card(\mathcal{F}) \;=\; \sum_{i=1}^{h} card(G * S_i) \;=\; r \cdot p^{n-k}m \;+\; p^{n-k}\sum_{i=r+1}^{h} p^{n_i-n+k}m_i$$

$$\Rightarrow\;\; m(r - 1 - pu) \;=\; \sum_{i=r+1}^{h} p^{n_i-n+k}m_i = p\sum_{i=r+1}^{h} p^{n_i-n+k-1}m_i \;\Rightarrow\; p \mid m(r-1-pu)$$

$$\Rightarrow\; p \mid m(r-1) \;\overset{(p \not| m)}{\Rightarrow}\; p \mid r-1 \;\Rightarrow\; r \equiv 1 \;\; (mod.\; p).\; \clubsuit$$

1.7. Homomorfismos de grupos

Ex. 104 *Demostrar que un grupo G es abeliano si y sólo si $f: G \to G$ tal que $f(x) = x^{-1}$ es un homomorfismo (de hecho se trata de un automorfismo, es decir un homomorfismo de un grupo en sí mismo que es biyectivo).*

$\equiv$

[$\Rightarrow$] Suponiendo que G es abeliano, veamos que la aplicación f anterior, que está bien definida, es un homomorfismo:

$$\forall x, y \in G, \quad f(xy) \;=\; (xy)^{-1} \;=\; y^{-1}x^{-1} \;=\; f(y)f(x) \;=\; (f(x)f(y).$$

[$\Leftarrow$] Suponiendo ahora que f es homomorfismo

$$\forall x, y \in G, \quad f(xy) = f(x)f(y) \;\Rightarrow\; (xy)^{-1} = x^{-1}y^{-1} = (yx)^{-1} \;\Rightarrow\; xy \;=\; yx. \;\clubsuit$$

Ex. 105 *Demostrar que un grupo G es abeliano si y sólo si $f: G \to G$ tal que $f(x) = x^2$ es un homomorfismo.*

$\equiv$

$$\forall x, y \in G, \quad f(xy) = f(x)f(y) \;\Leftrightarrow\; (xy)^2 = x^2y^2 \;\Leftrightarrow\; xyxy = xxyy \;\Leftrightarrow\; yx = xy. \;\clubsuit$$

Ex. 106 *Demostrar que un grupo G es abeliano si y sólo si $f: G \times G \to G$ tal que $f(x, y) = xy$ es un homomorfismo.*

$\equiv$

[$\Rightarrow$]

$$\forall (x, y), (a, b) \in G \times G, \quad f((x, y)(a, b)) = f(xa, yb) = xayb = xyab = f(x, y)f(a, b).$$

[$\Leftarrow$]

$$\forall x, y) \in G, \quad xy = f(x, y) = f((e, y)(x, e)) = f(e, y)f(x, e) = yx. \;\clubsuit$$

Ex. 107 *Determinar el número de homomorfismos distintos $f: \mathbf{Z}_m \to \mathbf{Z}_n$ en función de m, n.*

$\equiv$

Claramente, al hablar de los grupos $\mathbf{Z}_m, \mathbf{Z}_n$ se refieren a los grupos aditivos de las clases residuales (*mod.* m) y (*mod.* n), respectivamente. Consideramos el conjunto D de todos los enteros positivos que son divisores comunes de m y n, explícitamente

$$D \;=\; \{\, k \in \mathbf{N} \;:\; k|\, m, \;\; k \mid n \,\} \;=\; \{\, k \in \mathbf{N} \;:\; k \mid mcd(m, n)\}.$$

Para cada $k \in D$, definimos $A_k := \{[p]_n \in \mathbf{Z}_n \;:\; o([p]_n) = k\}$. Del Ejercicio 53, sabemos que, al ser $\mathbf{Z}_n$ cíclico, $card(A_k) = \Phi(k)$, siendo Φ la función de Euler. Veamos que, si llamamos

$$\mathcal{H}_{m,n} \;=\; \{\, f: \mathbf{Z}_m \to \mathbf{Z}_n \;:\; f \text{ es homomorfismo}\},$$

entonces $\mathcal{H}_{m,n}$ es equipotente a $\cup_{k\in D}A_k$: Para ello definimos la siguiente aplicación

$$\begin{array}{rcl}\psi & : & \cup_{k\in D}A_k \longrightarrow \mathcal{H}_{m,n} \\ & & [p]_n \ \to \ \psi([p]_n)([1]_m) \ = \ [p]_n.\end{array}$$

Notar que, para cada $[p]_n \in A_k$, $\psi([p]_n) \in \mathcal{H}_{m,n}$, ya que se trata del siguiente homomorfismo: Observar que, como $o([p]_n) = k \mid m$, se tiene que $[mp]_n = [0]_n$,

$\mathbf{Z}_m$		$\mathbf{Z}_n$
$[1]_m$	$\longrightarrow$	$[p]_n$
$[2]_m$	$\longrightarrow$	$[p]_n + [p]_n$
.....		
.....		
$[0]_m = [m]_m$	$\longrightarrow$	$[mp]_n = [0]_n$

ψ es inyectiva: Supongamos que $\psi([p]_n) = \psi([q]_n)$, con $[p]_n, [q]_n \in \cup_{k\in D}A_k$. Entonces

$$\left.\begin{array}{rcl}\psi([p]_n)([1]_m) & = & [p]_n \\ \psi([q]_n)([1]_m) & = & [q]_n\end{array}\right\} \ \Rightarrow \ [p]_n = [q]_n.$$

ψ es sobre: Sea $f \in \mathcal{H}_{m,n}$. Tomamos $[p]_n := f([1]_m)$. Veamos que $f = \psi([p]_n$. Evidente, ya que f y $\psi([p]_n)$ son homorfismos y

$$f([1]_m) \ = \ [p]_n \ = \ \psi([p]_n)([1]_m).$$

Finalmente, como los conjuntos A_k, $k \in D$, son disjuntos

$$card(\mathcal{H}_{m,n}) \ = \ card(\cup_{k\in D}A_k) \ = \ \sum_{k\in D} card(A_k) \ = \ \sum_{k \ \mid \ mcd(m,n)} \Phi(k) \ = \ mcd(m,n). \ \clubsuit$$

Ex. 108 *Demostrar que* $f : (\mathbf{R}, +) \to (\mathbf{R}^+, \cdot)$ *tal que* $f(x) = \mathrm{e}^x$, *con* $\mathbf{R}^+ =]0, +\infty[$, *es un isomorfismo. Quién es* f^{-1}*?*

$\equiv$

Un isomorfismo de grupos es un homomorfismo biyectivo. Así pues verifiquemos cada condición

f homomorfismo: Si $x, y \in \mathbf{R}$

$$f(x+y) \ = \ \mathrm{e}^{x+y} \ = \ \mathrm{e}^x \cdot \mathrm{e}^y \ = \ f(x) \cdot f(y).$$

f inyectivo:

$$x \in Ker\ f \ \Rightarrow \ 1 \ = \ f(x) \ = \ \mathrm{e}^x \ \Rightarrow \ x = 0.$$

f sobre: Dado $y \in \mathbf{R}^+$, todos sabemos resolver la ecuación $y = \mathrm{e}^x$. Tomanos pues $x = \log y$, que es un número real, ya que $y > 0$, tenemos que $f(x) = \mathrm{e}^x = y$.

Claramente

$$f^{-1}(x) \ = \ \log x, \quad x \in]0, +\infty[. \ \clubsuit$$

Ex. 109 *Demostrar que* $f : (\mathbf{Z}_{16}, +) \to (\mathbf{Z}'_{17}, \cdot)$ *tal que* $f([k]_{16}) = [3^k]_{17}$ *es un isomorfismo.*

$\equiv$

Recordemos que, al ser 17 número primo,

$$\mathbf{Z}'_{17} = \{ [1]_{17}, [2]_{17}, ..., [16]_{17} \}.$$

f bien definida: Sean $r, s \in \mathbf{Z}$ tales que $[r]_{16} = [s]_{16}$, veamos que $[3^r]_{17} = [3^s]_{17}$:

$$[r]_{16} = [s]_{16} \Rightarrow \exists p \in \mathbf{Z} \ / \ r - s = 16p \Rightarrow 3^r - 3^s = 3^s(3^{r-s} - 1)$$

$$= 3^s(3^{16p} - 1) = 3^s[(3^{16})^p - 1] = 3^s \cdot (3^{16} - 1)\frac{(3^{16})^p - 1}{3^{16} - 1}.$$

Luego, todo se reduce a ver que $3^{16} - 1$ es múltiplo de 17: Metiéndonos en $\mathbf{Z}_{17}$

$$[3^{16}]_{17} = ([3^4]_{17})^4 = ([81]_{17})^4 = ([13]_{17})^4 = (-[4]_{17})^4 = ([4]_{17})^4 = [256]_{17} = [1]_{17}$$

$$\Rightarrow [3^{16} - 1]_{17} = [0]_{17}.$$

f homomorfismo: Si $[r]_{16}, [s]_{16} \in \mathbf{Z}_{16}$

$$f([r]_{16} + [s]_{16}) = f([r + s]_{16}) = [3^{r+s}]_{17} = [3^r]_{17} \cdot [3^s]_{17} = f([r]_{16}) \cdot f([s]_{16}).$$

f inyectivo:

$$[r]_{16} \in Ker\ f \Rightarrow [1]_{17} = f([r]_{16}) = [3^r]_{17} \Rightarrow 17 \mid 3^r - 1 \overset{(probando:\ 0 \le r < 16)}{\Rightarrow} r = 0.$$

f sobre: Evidente, ya que los grupos $\mathbf{Z}_{16}$ y $\mathbf{Z}'_{17}$ tienen el mismo cardinal 16 y f es inyectiva. ♣

Ex. 110 *Demostrar que todo grupo de orden* 8 *es isomorfo a* $\mathbf{Z}_8$*, ó a* D_4*, ó a* Q*, ó a* $\mathbf{Z}_4 \times \mathbf{Z}_2$*, ó a* $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$.

$\equiv$

Si $o(G) = 8$, distinguimos tres casos según el cardinal de su generador

Caso 1. G cíclico. Suponiendo que $G = \langle x \rangle$, la aplicación $f : \mathbf{Z}_8 \to G$ tal que $f(\overline{k}) = x^k$ es un isomorfismo. Luego $G \cong \mathbf{Z}_8$.

Caso 2. G está generado por dos elementos. Así $G = \langle x, y \rangle$, $x \neq y$. Como $o(x)$,$o(y)$ son divisores de 4, podemos considerar dos subcasos

(2.1) $o(x) = o(y) = 4$. Veamos que $G \cong Q$ (grupo Quaternion). De la descripción del grupo Q (ver ejercicios anteriores), todo consiste en ver que: $x^2 = y^2$ y que $xyx = y$. Como $G = \{e, x, y, x^2, xy, x^3, x^2y, x^3y\}$ (ésto es fácil de verificar, por ejemplo, para ver

que $x^3 \neq xy$, componiendo por la izquierda con x^{-1} se tiene $x^2 = y$, pero ésto no puede ser ya que $y^2 = x^4 = e$ y $o(y)$ sería 2. Para ver que $y^2 = x^2$, se procede así:

$$\left.\begin{array}{l} Si\ x^2y^2 = x \rightarrow\ xy^2 = e,\ absurdo,\ pues\ x = xy^4 = y^2 \rightarrow\ G = \langle y\rangle \\ Si\ x^2y^2 = y \rightarrow\ x^2y = e,\ absurdo \\ Si\ x^2y^2 = x^2 \rightarrow\ y^2 = e,\ absurdo,\ ya\ que\ o(y) = 4 \\ Si\ x^2y^2 = xy \rightarrow\ xy = e,\ absurdo \\ Si\ x^2y^2 = x^3 \rightarrow\ y^2 = x,\ absurdo,\ ya\ que\ o(x) = 4 \\ Si\ x^2y^2 = x^2y \rightarrow\ y = e,\ absurdo \\ Si\ x^2y^2 = x^3y \rightarrow\ y = x,\ absurdo \end{array}\right\} \Rightarrow$$

$$\Rightarrow\ x^2y^2 = e\ \Rightarrow\ x^4y^2 = x^2\ \Rightarrow\ y^2 = x^2.$$

Análogamente se ve que $xyx = y$.

(2.2) $o(x) = 4$, $o(y) = 2$. Aquí se pueden dar dos posibilidades

(2.2.1) G tiene exactamente dos elementos de orden 4. Entonces G tiene dos elementos de orden 4 (x, x^3) y cinco de orden 2 (y, xy, y^2, x^2y, x^3y). Claramente, $G \cong D_4$ (grupo Dihédrico).

(2.2.2) G tiene más de dos elementos de orden 4. Ahora, como $o(y) = 2$, G tiene exactamente 4 elementos de orden 4 y 3 de orden 2. Es decir, $G \cong \mathbf{Z}_4 \times \mathbf{Z}_2$.

Caso 3. G está generado por tres elementos. Sea $G\langle x, y, z\rangle$. Obviamente $o(x) = o(y) = o(z) = 2$, por lo que $G = \{e, x, y, xy, xz, yz, xyz\}$, es decir, $G \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$. ♣

Ex. 111 *Si $o(G) = p^2$, p primo, demostrar que G es isomorfo a $\mathbf{Z}_{p^2}$ ó a $\mathbf{Z}_p \times \mathbf{Z}_p$.*

≡

Ahora la casuística es más sencilla que en el ejercicio precedente.

Caso 1. G cíclico. Es evidente que $G \cong \mathbf{Z}_{p^2}$.

Caso 2. G no cíclico. Entonces, al ser p primo, todo elemento distinto el neutro tiene orden p. Tomemos $x, y \in G\setminus\{e\}$ tales que $y \notin \langle x\rangle$ y consideremos el conjunto $H = \langle x\rangle\langle y\rangle$. Como el grupo G es abeliano (ejercicio 85), se tiene que H es un subgrupo de G. Además, al ser p primo y de la elección de x, y, se tiene que $\langle x\rangle \cap \langle y\rangle = \{e\}$,

$$o(H) \ = \ \frac{o(\langle x\rangle) \cdot o(\langle y\rangle)}{o(\langle x\rangle \cap \langle y\rangle)} \ = \ p^2.$$

Por tanto, $H = G$ y podemos definir

$$\begin{array}{rcl} f & : & \mathbf{Z}_p \times \mathbf{Z}_p \longrightarrow\ G \\ & & (\overline{r}, \overline{s}) \rightarrow\ f(\overline{r}, \overline{s}) = x^r y^s \end{array}$$

f bien definida: Sean $\overline{r} = \overline{r'}$ y $\overline{s} = \overline{s'}$. Entonces $r' - r = np$, $s' - s = n'p$, $n, n' \in \mathbf{Z}$. Así

$$x^{r'}y^{s'} \ = \ x^{r+np}y^{s+n'p} \ = \ x^r y^s.$$

f homomorfismo: Recordando que G es abeliano

$$f((\overline{r}, \overline{s}) + (\overline{a}, \overline{b})) \ = \ f(\overline{r+a}, \overline{s+b}) \ = \ x^{r+a}y^{s+b} \ = \ x^r y^s x^a y^b \ = \ f(\overline{r}, \overline{s})f(\overline{a}, \overline{b}).$$

f inyectivo: Si $(\overline{r}, \overline{s}) \in Ker\ f$, entonces

$$e = f(\overline{r}, \overline{s}) = x^r y^s \Rightarrow x^r = y^{-s} \in \langle x \rangle \cap \langle y \rangle = \{e\} \Rightarrow \overline{r} = \overline{s} = \overline{0}. \clubsuit$$

Ex. 112 *Sea G el grupo $(]-1,1[, \bullet)$, siendo*

$$x \bullet y = \frac{x+y}{1+xy}, \qquad x, y \in]-1,1[.$$

Demostrar que G es isomorfo al grupo aditivo $\mathbf{R}$.

$\equiv$

Ya vimos en el Lema 2 correspondiente a la resolución del Ex. 11 que este grupo $G = (]-1,1[, \bullet)$ es un grupo abeliano de neutro 0 y tal que, si $x \in G$, su simétrico es $-x$. Antes de definir la aplicación isomórfica de G en $(\mathbf{R}, +)$, vamos a recordar algunas propiedades referente a las funciones hiperbólicas:

1) Función coseno hiperbólico: Se define en toda la recta real como

$$\cosh x = \frac{e^x + e^{-x}}{2}, \qquad x \in \mathbf{R}.$$

2) Función seno hiperbólico: Se define en toda la recta real como

$$\sinh x = \frac{e^x - e^{-x}}{2}, \qquad x \in \mathbf{R}.$$

3) Función tangente hiperbólica: Se define en toda la recta real como

$$\tanh x = \frac{\sinh x}{\cosh x}, \qquad x \in \mathbf{R}.$$

Propiedades

1) $\cosh^2 x - \sinh^2 x = 1.$

2)

$$\cosh(x+y) = \cosh x \cdot \cosh y + \sinh x \cdot \sinh y$$

$$\sinh(x+y) = \sinh x \cdot \cosh y + \cosh x \cdot \sinh y$$

$$\tanh(x+y) = \frac{\tanh x + \tanh y}{1 + \tanh x \cdot \tanh y}.$$

La tercera igualdad de la propiedad 2 anterior nos indica que la función que nos interesa es $f(x) = \tanh x$, así que vamos a estudiar su comportamiento analítico:

$$\lim_{x\to+\infty} f(x) = \lim_{x\to+\infty} \frac{e^x - e^{-x}}{e^x + e^{-x}} = \lim_{x\to+\infty} \frac{e^{2x}-1}{e^{2x}+1} \overset{(L'Hôpital)}{=} \lim_{x\to+\infty} \frac{2e^{2x}}{2e^{2x}} = 1$$

$$\lim_{x\to-\infty} f(x) = \lim_{x\to-\infty} \frac{e^x - e^{-x}}{e^x + e^{-x}} = \lim_{x\to-\infty} \frac{e^{2x}-1}{e^{2x}+1} = \frac{0-1}{0+1} = -1.$$

Además, derivando

$$f'(x) = \frac{1}{\cosh^2 x} = \frac{(e^x + e^{-x})^2}{4} > 0 \Rightarrow f(x) \text{ es estrict. creciente.}$$

Así pues, consideremos la función

$$\begin{array}{rccc} f : (\mathbf{R}, +) & \longrightarrow & (G, \bullet) \\ x & \to & f(x) = \tanh x. \end{array}$$

Claramente, f está bien definida, ya que, $\forall x \in \mathbf{R}$, $-1 < f(x) < 1$. Al ser estrictamente creciente, f es inyectiva y, al tratarse de una función continua y tener los límites que tiene cuando x tiende a $\pm\infty$, se deduce que f también es sobre, es decir f es biyectiva. Por lo tanto, sólo nos falta ver que f es un homomorfismo de grupos: Dados $x, y \in \mathbf{R}$, de la tercera igualdad de la propiedad 2 anterior

$$f(x+y) = \tanh(x+y) = \frac{\tanh x + \tanh y}{1 + \tanh x \cdot \tanh y} = \frac{f(x) + f(y)}{1 + f(x) \cdot f(y)} = f(x) \bullet f(y). \clubsuit$$

Ex. 113 *Demostrar que todo grupo abeliano finito es isomorfo a un producto directo de grupos cíclicos.*

≡

Sea G un grupo abeliano finito y sea su orden

$$o(G) = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_m^{n_m}.$$

Del $T1S$, para cada $i = 1, 2, ..., m$, existe un sugrupo H_i tal que $o(H_i) = p_i^{n_i}$. Todo se reduce a ver que $G = H_1 H_2 ... H_m$:

Como G es abeliano sabemos que $H_1 H_2 ... H_m$ es un subgrupo. Además, para cada $i = 1, 2, ..., m$,

$$o(H_i \cap (\prod_{j \neq i} H_j)) = 1, \text{ ya que ha de dividir a } mcd(p_1^{n_1}, p_2^{n_2}, ..., p_m^{n_m}) = 1)$$

$$\Rightarrow H_i \cap (\prod_{j \neq i} H_j) = \{e\}.$$

Por tanto

$$o(H_1 H_2 ... H_m) = o(H_1) o(H_2) ... o(H_m) = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_m^{n_m} = o(G) \Rightarrow H_1 H_2 ... H_m = G.$$

Finalmente, considerando el subgrupo H_1 cuyo orden es $p_1^{n_1}$. Del teorema de Cauchy, existe un elemento $x_1 \in H_1$, con orden p_1, tal que $H_1 = \langle x_1 \rangle \cdot H_1'$. Aplicando de nuevo el teorema de Cauchy a H_1', existe otro elemento x_2 de orden p_1 de modo que $H_1' = \langle x_2 \rangle H_1''$. Procediendo de este modo se hallan $x_1, x_2, ..., x_{n_1} \in H_1$ tales que

$$H_1 = \langle x_1 \rangle \cdot \langle x_2 \rangle \cdot \ldots \cdot \langle x_{n_1} \rangle.$$

Llamando $x_{11} := x_1$, $x_{12} := x_2, ..., x_{1n_1} := x_{n_1}$ y procediendo de manera análoga para los subgrupos restantes $H_2, ..., H_n$, obtenemos elementos x_{ij}, $1 \leq i \leq m$, $1 \leq j \leq n_i$, tales que

$$G = H_1 \cdot H_2 \cdot ... \cdot H_m = \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n_i}} \langle x_{ij} \rangle. \ \clubsuit$$

Ex. 114 *Dado un grupo G, sea $A(G)$ el conjunto de los automorfismos de G, es decir,*

$$A(G) = \{ f : G \to G \ : \ f \text{ es un isomorfismo } \}.$$

a) Demostrar que $A(G)$ es un grupo para la composición de aplicaciones (el grupo de los automorfismos).

b) Para cada $a \in G$, definimos

$$\begin{array}{rccl} h_a : & G & \longrightarrow & G \\ & x & \to & h_a(x) = a^{-1}xa \ . \end{array}$$

Si llamamos $I(G) = \{ h_a \ : \ a \in G \}$, demostrar que $I(G)$ es un subgrupo normal de $A(G)$ (el subgrupo de los automorfismos internos).

$\equiv$

a) Como $A(G) \subset \Sigma(G)$, donde $\Sigma(G)$ es el grupo de las biyecciones de G en sí mismo para la composición, todo se reduce a verificar que: Si $f, g \in A(G)$, entonces $f \circ g \in A(G)$ y $f^{-1} \in A(G)$, dados $x, y \in G$,

$$\left.\begin{array}{l} f \circ g \text{ es biyectiva} \\ (f \circ g)(xy) = f[g(xy)] = f[g(x)g(y)] = f[g(x)]f[g(y)] = (f \circ g)(x)(f \circ g)(y) \end{array}\right\}$$

$$\Rightarrow \ f \circ g \ \in \ A(G).$$

Además

$$\left.\begin{array}{l} f^{-1} \text{ es biyectiva} \\ f[f^{-1}(xy)] = xy = f[f^{-1}(x)]f[f^{-1}(y)] = f[f^{-1}(x)f^{-1}(y)] \to f^{-1}(xy) = f^{-1}(x)f^{-1}(y) \end{array}\right\}$$

$$\Rightarrow f^{-1} \in A(G).$$

b) Para comprobar que $I(G)$ es un subgrupo normal de $A(G)$ hemos de demostrar tres cosas:

(b.1) $I(G) \subset A(G)$: Sea $f \in I(G)$. Por definición, existe $a \in G$ tal que $f = h_a$. Veamos que h_a es biyectiva: Si $h_a(x) = h_a(y)$, entonces $a^{-1}xa = a^{-1}ya$ y, componiendo con a por la izquierda y con a^{-1} por la derecha, se deduce que $x = y$, es decir h_a es inyectiva. Ahora, si $y \in G$, tomando $x := aya^{-1} \in G$, es fácil verificar que $h_a(x) = y$, luego h_a es sobre. Sólo queda demostrar que h_a es homomorfismo: Sean $x, y \in G$,

$$h_a(xy) = a^{-1}xya = (a^{-1}xa)(a^{-1}ya) = h_a(x)h_a(y).$$

(b.2) $I(G)$ es subgrupo de $A(G)$: Como antes, si $a, b \in G$, basta con probar que $h_a \circ h_b^{-1} \in I(G)$: Para ello, comprobemos que $h_a \circ h_b^{-1} = h_{b^{-1}a}$, si $x \in G$,

$$(h_a \circ h_b^{-1})(x) = h_a[h_b^{-1}(x)] = h_a(bxb^{-1}) = a^{-1}(bxb^{-1})a = (b^{-1}a)^{-1}x(b^{-1}a) = h_{b^{-1}a}(x).$$

(b.3) $I(G)$ es subgrupo normal de $A(G)$: Hay que ver que, si $f \in A(G)$, entonces $f \circ I(G) = I(G) \circ f$: Para ello, sea h_a, $a \in G$, un elemento cualquiera de $I(G)$. Dado $x \in G$

$$(f \circ h_a)(x) = f(a^{-1}xa) = f(a)^{-1}f(x)f(a) = h_{f(a)}[f(x)] = (h_{f(a)} \circ f)(x)$$

$$\Rightarrow\ f \circ h_a = h_{f(a)} \circ f\ \Rightarrow\ f \circ I(G)\ \subset\ I(G) \circ f.$$

$$(h_a \circ f)(x) = a^{-1}f(x)a = f[f^{-1}(a^{-1})]f(x)f[f^{-1}(a)] = f[f^{-1}(a^{-1})xf^{-1}(a)] = f[f^{-1}(a)^{-1}xf^{-1}(a)]$$

$$= (f \circ h_{f^{-1}(a)})(x)\ \Rightarrow\ h_a \circ f = f \circ h_{f^{-1}(a)}\ \Rightarrow\ I(G) \circ f\ \subset\ f \circ I(G).\ \clubsuit$$

Ex. 115 *Dado un grupo G, sea $Z(G)$ su centro y sea $I(G)$ el subgrupo normal de $A(G)$ introducido en el ejercicio anterior. Demostrar que $G/Z_G \cong I(G)$.*

$\equiv$

Usando la notación del ejercicio anterior, definimos

$$\begin{array}{rccl} \psi & : & G & \longrightarrow & I(G) \\ & & a & \to & \psi(a) = h_a^{-1},\ i.e.,\ \psi(a)(x) = axa^{-1},\quad x \in G. \end{array}$$

ψ bien definida: Obvio, pues $\forall a \in G,\ \psi(a) = h_a^{-1} \in I(G)$, como vimos antes.
ψ homomorfismo: $\forall a, b, x \in G$,

$$\psi(ab)(x)\ =\ h_{ab}^{-1}(x)\ =\ abx(ab)^{-1} = abxb^{-1}a^{-1}$$

$$= ah_b^{-1}(x)a^{-1} = h_a^{-1}(h_b^{-1}(x)) = (h_a^{-1} \circ h_b^{-1})(x).$$

Por tanto $\psi(ab) = \psi(a) \circ \psi(b)$.
ψ sobre: $\forall f \in I(G)$, existe $a \in G$ tal que $f = h_a$. Entonces

$$\forall x \in G,\quad f(x) = h_a(x) = a^{-1}xa = h_{a^{-1}}^{-1}(x)\ \Rightarrow\ f = h_{a^{-1}}^{-1} = \psi(a^{-1}).$$

Aplicando el Primer Teorema del Isomorfismo: $G/Ker(\psi) \cong \psi(G) = I(G)$. Por tanto, todo se reduce a ver que $Ker(\psi) = Z_G$:

[$\subset$] Si $a \in Ker(\psi)$, como $id_G = \psi(a) = h_a^{-1}$, se tiene que, $\forall x \in G$,

$$x\ =\ axa^{-1}\ \to\ ax\ =\ xa\ \ \Rightarrow\ \ a \in Z_G.$$

[$\supset$] Si $a \in Z_G$, como $ax = xa$, $\forall x \in G$, tenemos que

$$\psi(a)(x)\ =\ h_a^{-1}(x) = axa^{-1} = xaa^{-1} = x\ \Rightarrow\ \ \psi(a) = id_G,\ i.e.\ a \in Ker(\psi).\ \clubsuit$$

Ex. 116 *Dado un grupo finito G, demostrar que si $o(G) > 2$, entonces $o(A(G)) > 1$.*

$\equiv$

Distinguimos dos casos

Caso 1: G no es abeliano. Entonces existen dos elementos $a, b \in G$ tales que $ab \neq ba$. Para ver que $o(I(G)) > 1$, todo se reduce a ver que $h_a \neq id_G$. Evidente, de lo contrario

$$b = h_a(b) = a^{-1}ba \rightarrow ab = ba. \quad \text{Absurdo}$$

Caso 2: G es abeliano. Ahora consideramos dos subcasos

(2.1) G tiene algún elemento de orden ≥ 3. Sea $a \in G$ tal que $o(a) \geq 3$. Del Ex. 104, sabemos que, al ser G abeliano, la aplicación $f(x) = x^{-1}$, $x \in G$, es un automorfismo de G, es decir, $f \in A(G)$. Como antes, todo consiste en ver que $f \neq id_G$. De lo contrario

$$a^{-1} = f(a) = a \rightarrow a^2 = e. \quad \text{Absurdo}$$

(2.2) Todo elemento de G distinto del neutro tiene orden 2. Consideremos un sistema minimal de generadores de G dado por

$$S = \{ a_1, a_2, ..., a_n\}.$$

Afirmamos que $n \geq 2$, de lo contrario $S = \{a_1\}$ implicaría que $G = \{e, a_1\}$, lo que contradice la hipótesis de $o(G) > 2$. Por tanto sabemos que $a_1 \neq a_2$. Sea ahora $f : G \rightarrow G$ el homomorfismo tal que

$$f(a_1) = a_2, \quad f(a_2) = a_1, \quad f(a_i) = a_i, \quad 3 \leq i \leq n.$$

Es decir, como para cada $x \in G$, al ser de orden 2 máximo, existen $m_1, m_2, ..., m_n \in \{0, 1\}$ de modo que $x = a_1^{m_1}a_2^{m_2}...a_n^{m_n}$, se tiene que $f(x) = a_2^{m_1}a_1^{m_2}a_3^{m_3}...a_n^{m_n}$, que es claramente un homomorfismo. Veamos que es inyectivo

$$f(x) = e \rightarrow a_2^{m_1}a_1^{m_2}a_3^{m_3}...a_n^{m_n} = e \rightarrow m_1 = m_2 = ... = m_n = 0 \rightarrow x = e$$

$$\Rightarrow Ker(f) = \{e\}.$$

Al tratarse de un grupo finito está claro que $f \in A(G)$. Para terminar sólo queda ver que $f \neq id_G$: Inmediato, ya que $f(a_1) = a_2 \neq a_1$. ♣

Ex. 117 *Determinar el número de automorfismos distintos de* $\mathbf{Z}_n$ *y de* D_n.

$\equiv$

Veamos que $o(A(\mathbf{Z}_n)) = \Phi(n)$, siendo Φ la función de Euler que introducíamos en la Nota 5 del Ex. 52. Para ello, basta con demostrar que $A(\mathbf{Z}_n)$ es equipotente con $\mathbf{Z}'_n$, donde $\mathbf{Z}'_n = \{\overline{k} \in \mathbf{Z}_n : mcd(k, n) = 1\}$ (recordar que $card(\mathbf{Z}'_n) = \Phi(n)$). Así pues, definimos

$$\begin{array}{rcl} \psi : A(\mathbf{Z}_n) & \longrightarrow & \mathbf{Z}'_n \\ f & \rightarrow & \psi(f) = f(\overline{1}). \end{array}$$

ψ bien definida: Como f es isomorfismo

$$\langle f(\overline{1})\rangle = f(\mathbf{Z}_n) = \mathbf{Z}_n,$$

ello implica que $f(\overline{1})$ es un generador de $\mathbf{Z}_n$, por lo que $f(\overline{1}) \in \mathbf{Z}'_n$.
ψ inyectiva: Si $f, g \in A(\mathbf{Z}_n)$ son tales que $\psi(f) = \psi(g)$, entonces $f(\overline{1}) = g(\overline{1})$, lo que implica, al ser isomorfismos y ser $\overline{1}$ generador de $\mathbf{Z}_n$, que $f = g$.
ψ sobre: Sea $\overline{k} \in \mathbf{Z}'_n$. Definiendo $f(\overline{i}) = \overline{ki}$, $\overline{i} \in \mathbf{Z}_n$, se obtiene un homomorfismo de $\mathbf{Z}_n$ en sí mismo. Además

$$f(\overline{i}) = \overline{0} \ \rightarrow \ n| \ ki \overset{mcd(k,n)=1}{\rightarrow} \ n| \ i \ \rightarrow \ \overline{i} = \overline{0},$$

es decir, f es inyectiva y entonces $f \in A(\mathbf{Z}_n)$, como queríamos. Obviamente $\psi(f) = \overline{k}$.

Veamos que $o(A(D_n)) = n \cdot \Phi(n)$. para ello, recordemos de ejercicios anteriores que el grupo dihédrico se descompone como

$$D_n \ = \ \{ \ e, \rho, \rho^2, ..., \rho^{n-1} \} \ \cup \ \{ \ \sigma, \rho\sigma, \rho^2\sigma, ..., \rho^{n-1}\sigma \}.$$

Llamando $G_n := \{ \ e, \rho, \rho^2, ..., \rho^{n-1} \}$ y $A_n := \{ \ \sigma, \rho\sigma, \rho^2\sigma, ..., \rho^{n-1}\sigma \}$, siendo ρ una rotación de ángulo $\frac{2\pi}{n}$ y σ una simetría axial. Claramente G_n es un grupo isomorfo a $\mathbf{Z}_n$ y $D_n = G_n \cup A_n$. Por tanto, de la primera parte de este ejercicio, como $o(A(G_n)) = o(A(\mathbf{Z}_n)) = \Phi(n)$, todo se reduce a probar que los conjuntos $A(D_n))$ y $A_n \times A(G_n)$ son equipotentes. Para ello, definimos

$$\begin{array}{rcl} \psi \ : \ A(D_n)) & \longrightarrow & A_n \times A(G_n) \\ f & \rightarrow & \psi(f) = (f(\sigma), f_{|G_n}). \end{array}$$

ψ bien definida: $\forall f \in A(D_n)$, al ser f un isomorfismo $f(\sigma)$ tiene el mismo orden que σ, es decir 2, luego $f(\sigma) \in A_n$. Además, si llamamos $h := f_{|G_n}$, es evidente que h es un homomorfismo inyectivo tal que $h(G_n) = h(\langle \rho \rangle) = \langle h(\rho) \rangle \subset G_n$, ya que $h(\rho) = f(\rho)$ tiene orden n. Obviamente, $h(G_n) = G_n$, lo que prueba que $h \in A(G_n)$.
ψ inyectiva: Si $f, g \in A(D_n)$ son tales que $\psi(f) = \psi(g)$, entonces

$$(f(\sigma), f_{|G_n}) = (g(\sigma), g_{|G_n}) \rightarrow \left\{ \begin{array}{l} f(\sigma) = g(\sigma) \\ f_{|G_n} = g_{|G_n} \end{array} \right\} \ \Rightarrow \ f = g.$$

ψ sobre: Si $\rho^i\sigma \in A_n$, $h \in A(G_n)$, definimos

$$f \ : \ D_n \longrightarrow \ D_n \quad \text{tal que} \ \left\{ \begin{array}{l} f(\rho^k) = h(\rho^k), \\ f(\rho^k\sigma) = \rho^{k+i}\sigma \end{array} \right\}, \ 0 \leq k \leq n-1.$$

Entonces $f \in A(D_n)$ y claramente $\psi(f) = (\rho^i\sigma, h)$. ♣

Ex. 118 *Dado un grupo G, H es un subgrupo característico de G siempre que, $\forall f \in A(G)$, se tiene que $f(H) = H$.*

1) *Demostrar que si H es un subgrupo característico de G y K es un subgrupo característico de H, entonces K es un subgrupo característico de G.*
2) *Demostrar que si H es un subgrupo normal de G y K es un subgrupo característico de H, entonces K es un subgrupo normal de G.*

≡
1) Dado $f \in A(G)$, como $f(H) = H$, tenemos que $f_{|H} \in A(H)$. Por tanto, al ser K un subgrupo característico de H, se tiene $f(K) = f_{|H}(K) = K$.
2) Dado $a \in G$, consideramos el automorfismo h_a definido por $h_a(x) = a^{-1}xa$, $x \in G$. Entonces $h_a \in A(G)$. Como H es normal en G, sabemos que $a^{-1}Ha = H$, de donde

$$H \;=\; a^{-1}Ha \;=\; h_a(H).$$

Ello implica que $h_{a_{|H}} \in A(H)$. Como K es subgrupo característico de H, tenemos que

$$K \;=\; h_{a_{|H}}(K) \;=\; h_a(K) \;=\; a^{-1}Ka,$$

lo que nos dice que K es normal en G. ♣

Ex. 119 *Determinar el grupo de automorfismos de* $\mathbf{Z}_2 \times \mathbf{Z}_2$, *i.e.,* $A(\mathbf{Z}_2 \times \mathbf{Z}_2)$.

≡
Veamos que

$$A(\mathbf{Z}_2 \times \mathbf{Z}_2) \;=\; \{\, f : \mathbf{Z}_2 \times \mathbf{Z}_2 \to \mathbf{Z}_2 \times \mathbf{Z}_2 \;:\; f \text{ es biyectiva, } f(\overline{0},\overline{0}) = (\overline{0},\overline{0})\}.$$

Por comodidad, escribimos

$$\mathbf{Z}_2 \times \mathbf{Z}_2 \;=\; \{\, e,\; x_1,\; x_2,\; x_3\}, \quad \text{siendo } e = (\overline{0},\overline{0}), x_1 = (\overline{1},\overline{0}), x_2 = (\overline{0},\overline{1}), x_3 = (\overline{1},\overline{1}).$$

[⊂] Obvio, pues si $f \in A(\mathbf{Z}_2 \times \mathbf{Z}_2)$, entonces f es biyectiva y $f(e) = e$.
[⊃] Sea $f : \mathbf{Z}_2 \times \mathbf{Z}_2 \to \mathbf{Z}_2 \times \mathbf{Z}_2$ tal que f es biyectiva, $f(\overline{0},\overline{0}) = (\overline{0},\overline{0})$. Entonces

$$f(\mathbf{Z}_2 \times \mathbf{Z}_2) \;=\; \{f(e), f(x_1), f(x_2), f(x_3)\} \;=\; \{e, f(x_1), f(x_2), f(x_3)\}.$$

Para ver que $f \in A(\mathbf{Z}_2 \times \mathbf{Z}_2)$, basta con verificar que f es homomorfismo, lo que se reduce a comprobar que, ya que $f(e) = e$, para $i, j \in \{1,2,3\}$, $f(x_ix_j) = f(x_i)f(x_j)$:

$$\text{Si } i = j \;\to\; \begin{cases} f(x_ix_j) = f(x_i^2) = f(e) = e \\ f(x_i)f(x_j) = f(x_i)^2 = e \end{cases}$$
$$\text{Si } i \neq j \;\to\; \begin{cases} f(x_ix_j) = f(x_k),\; k \notin \{i,j\} \\ f(x_i)f(x_j) = f(x_k), \text{ al ser biyectiva. } ♣ \end{cases}$$

Nota 9 Observar que $\mathbf{Z}_2 \times \mathbf{Z}_2$ es isomorfo al Viergruppe de Klein. Además, como los elementos de $A(\mathbf{Z}_2 \times \mathbf{Z}_2)$ son las biyecciones de $\mathbf{Z}_2 \times \mathbf{Z}_2$ en sí mismo que dejan fijo al par $(\overline{0},\overline{0})$, tenemos que el orden de $A(\mathbf{Z}_2 \times \mathbf{Z}_2)$ es

$$o(A(\mathbf{Z}_2 \times \mathbf{Z}_2)) \;=\; 3! \;=\; 6.$$

Ex. 120 *Consideremos el grupo aditivo real* $\mathbf{R}$ *y el grupo multiplicativo complejo* $\mathbf{C}^* = \mathbf{C} \setminus \{0\}$. *Efectuar la descomposición canónica del homomorfismo de Euler*

$$\begin{array}{rccl} f & : & \mathbf{R} & \longrightarrow & \mathbf{C}^* \\ & & x & \to & f(x) \;=\; \mathrm{e}^{2\pi ix}. \end{array}$$

$\equiv$

Primero comprobemos que se trata de un homomorfismo de grupos: Si $x, y \in \mathbf{R}$, entonces

$$f(x+y) \;=\; \mathrm{e}^{2\pi i(x+y)} \;=\; \mathrm{e}^{2\pi ix+2\pi iy} = \; \mathrm{e}^{2\pi ix} \cdot \mathrm{e}^{2\pi iy} = \; f(x) \cdot f(y).$$

Efectuar la descomposición canónica de este homomorfismo consiste en describir cada uno de los ingredientes del siguiente diagrama conmutativo

$$\begin{array}{ccc} \mathbf{R} & \xrightarrow{f} & \mathbf{C}^* \\ p \downarrow & & \uparrow\, i \\ \frac{\mathbf{R}}{Ker(f)} & \xrightarrow{\widetilde{f}} & f(\mathbf{R}). \end{array}$$

Como ya sabemos quien es f, procedemos a describir los restantes homomorfismos. Antes determinamos el $Ker(f)$

$$x \in Ker(f) \;\leftrightarrow\; f(x) = 1 \;\leftrightarrow\; \mathrm{e}^{2\pi ix} = 1 \;\leftrightarrow\; \cos(2\pi x) = 1 \;\leftrightarrow\; x \in \mathbf{Z} \;\Rightarrow\; Ker(f) = \mathbf{Z}.$$

Es fácil ver que el rango de f es

$$f(\mathbf{R}) \;=\; \{\, z \in \mathbf{C} \;:\; |\, z \,| \,=\, 1\} \;\text{(circunferencia unidad compleja)}.$$

La aplicación $p : \mathbf{R} \to \mathbf{R}/Ker(f) = \mathbf{R}/\mathbf{Z}$ es la proyección canónica, i.e., $p(x) = x + \mathbf{Z}$. Mediante $i \;:\; f(\mathbf{R}) \to \mathbf{C}^*$ representamos la identidad, i.e., $i(z) = z$. Finalmente, la aplicación $\widetilde{f} \;:\; \mathbf{R}/\mathbf{Z} \to f(\mathbf{R})$ es el isomorfismo dado por $\widetilde{f}(x+\mathbf{Z}) \;=\; f(x)$. De manera que el diagram anterior conmuta, es decir

$$i \circ \widetilde{f} \circ p \;=\; f \;. \clubsuit$$

Ex. 121 *Dado el grupo G, consideramos el homomorfismo $\psi : G \to A(G)$ tal que, para $a \in G$, $\psi(a) = h_a$, siendo h_a el automorfismo de G dado por $h_a(x) = a^{-1}xa$, $x \in G$. Hallar la descomposición canónica de ψ.*

$\equiv$

Como hicimos en el ejercicio previo, buscamos determinar cada uno de los componentes del siguiente diagrama conmutativo

$$\left\{ \begin{array}{ccc} G & \xrightarrow{\psi} & A(G) \\ p \downarrow & & \uparrow\, i \\ \frac{G}{Ker(\psi)} & \xrightarrow{\widetilde{\psi}} & \psi(G) \end{array} \right\} \;\Leftrightarrow\; \psi \;=\; i \circ \widetilde{\psi} \circ i \;.$$

Ya vimos en en un ejercicio anterior que $Ker(\psi) = Z_G$ y que $\psi(G) = I(G)$, donde $I(G)$ es

el subgrupo de los automorfismos internos de G, i.e., los de la forma h_a, $a \in G$. Así pues

$$\begin{array}{rcl} p & : & G \overset{proy.can.}{\longrightarrow} \frac{G}{Z_G} \\ & & x \to p(x) = xZ_G \end{array}$$

$$\begin{array}{rcl} i & : & I(G) \overset{iny.can.}{\longrightarrow} A(G) \\ & & f \to i(f) = f \end{array}$$

$$\begin{array}{rcl} \widetilde{\psi} & : & \frac{G}{Z_G} \overset{isom.}{\longrightarrow} I(G) \\ & & xZ_G \to \widetilde{\psi}(xZ_G) = \psi(x) = h_x. \ \clubsuit \end{array}$$

Ex. 122 *Dados $m, n \in \mathbf{N}$, consideramos el homomorfismo $f : \mathbf{Z} \to \mathbf{Z}_m$ dado por $f(k) = \overline{nk}$, $k \in \mathbf{Z}$. Hallar la descomposición canónica de f.*

$\equiv$

De nuevo a partir del diagrama conmutativo

$$\left\{ \begin{array}{ccc} \mathbf{Z} & \xrightarrow{f} & \mathbf{Z}_m \\ p \downarrow & & \uparrow i \\ \frac{\mathbf{Z}}{Ker(f)} & \xrightarrow{\widetilde{f}} & f(\mathbf{Z}) \end{array} \right\} \quad \Leftrightarrow \quad f = i \circ \widetilde{f} \circ i \, ,$$

hallamos sus componentes.

Veamos que $Ker(f) = \frac{m}{mcd(m,n)}\mathbf{Z}$:

$$k \in Ker(f) \leftrightarrow f(k) = \overline{0} \leftrightarrow \overline{kn} = \overline{0} \leftrightarrow m | \, kn \leftrightarrow \frac{\frac{nk}{mcd(m,n)}}{\frac{m}{mcd(m,n)}} = \frac{nk}{m} \in \mathbf{Z} \leftrightarrow \frac{m}{mcd(m,n)} \, | \, k.$$

Claramente $f(\mathbf{Z}) = \{\overline{kn} : \ k \in \mathbf{Z}\} = n\mathbf{Z}_m$.

$$\begin{array}{rcl} p & : & \mathbf{Z} \overset{proy.can.}{\longrightarrow} \frac{\mathbf{Z}}{\frac{m}{mcd(m,n)}\mathbf{Z}} = \mathbf{Z}_{\frac{m}{mcd(m,n)}} \\ & & k \to p(k) = \overline{k} \end{array}$$

$$\begin{array}{rcl} i & : & n\mathbf{Z}_m \overset{iny.can.}{\longrightarrow} \mathbf{Z}_m \\ & & n\overline{k} \to i(n\overline{k}) = \overline{nk} \end{array}$$

$$\begin{array}{rcl} \widetilde{f} & : & \mathbf{Z}_{\frac{m}{mcd(m,n)}} \overset{isom.}{\longrightarrow} n\mathbf{Z}_m \\ & & \overline{k} \to \widetilde{f}(\overline{k}) = f(\overline{k}) = \overline{kn}. \ \clubsuit \end{array}$$

Ex. 123 *Sea U el grupo multiplicativo de la circunferencia unidad compleja. Dado $n \in \mathbf{N}$, sea $f : U \to U$ el homomorfismo dado por $f(z) = z^n$. Hallar la descomposición canónica de f.*

$\equiv$

Otra vez hacemos el diagrama y determinamos sus ingradientes.

$$\left\{ \begin{array}{ccc} U & \xrightarrow{f} & U \\ p\downarrow & & \uparrow i \\ \frac{U}{Ker(f)} & \xrightarrow{\tilde{f}} & f(U) \end{array} \right\} \Leftrightarrow f = i \circ \tilde{f} \circ i \, .$$

Utilizando la forma polar de un número complejo

$$z = 1_\alpha \in Ker(f) \leftrightarrow 1_{n\alpha} = z^n = f(z) = 1 = 1_0$$

$$\leftrightarrow n\alpha \in \{2k\pi : k \in \mathbf{Z}\} \leftrightarrow \alpha \in \{0, \frac{2\pi}{n}, 2\frac{2\pi}{n}, ..., (n-1)\frac{2\pi}{n}\} \leftrightarrow z = 1_\alpha \in \{1, 1_{\frac{2\pi}{n}}, ..., 1_{\frac{2(n-1)\pi}{n}}\},$$

i.e., llamando U_n al conjunto de las raices n – ésimas de la unidad, $Ker(f) = U_n$.

Veamos ahora que $f(U) = U$: Como la inclusión directa es evidente, demostramos la recíproca

$\forall z \in U$, $\exists \alpha \in]-\pi, \pi]$ tal que $z = 1_\alpha$. Tomando $w = 1_{\frac{\alpha}{n}} \in U \Rightarrow f(w) = w^n = (1_{\frac{\alpha}{n}})^n = 1_\alpha = z$.

Así

$$\begin{array}{rcl} p : U & \xrightarrow{proy.can.} & \frac{U}{U_n} \\ z & \to & p(z) = zU_n \end{array}$$

$$\begin{array}{rcl} i : U & \xrightarrow{iny.can.} & U \\ z & \to & i(z) = z \end{array}$$

$$\begin{array}{rcl} \tilde{f} : \frac{U}{U_n} & \xrightarrow{isom.} & U \\ zU_n & \to & \tilde{f}(zU_n) = f(z) = z^n. \end{array} \clubsuit$$

Nota 10 Observar que este ejercicio demuestra que $U \cong \frac{U}{U_n}$.

1.8. Grupos resolubles

Ex. 124 *Demostrar que todo grupo finito posee una serie de composición.*

$\equiv$

Recordemos primero que el concepto de serie de composición de un grupo G se refiere a una expresión de la forma

$$\{e\} = H_0 \preceq H_1 \preceq ... \; H_{n-1} \preceq H_n = G, \qquad (*)$$

donde el símbolo $H_i \preceq H_{i+1}$ indica que H_i es un subgrupo normal de H_{i+1}, $0 \leq i \leq n-1$, y $S = \{H_0, H_1, ..., H_{n-1}, H_n\}$ es maximal respecto de la inclusión.

Si $G = \{e\}$, es obvio que $S = \{\{e\}\}$ es una serie de composición. Podemos suponer por tanto que $o(G) > 1$. Consideremos la familia

$$\mathcal{N} := \{ S^* : S^* \text{ es una serie normal de } G\},$$

donde por serie normal entendemos una cadena finita análoga a $(*)$ sin necesidad de ser maximal. Como $S_0 = \{H_0 = \{e\}, H_1 = G\}$ es una serie normal de G, queda claro que $S_0 \in \mathcal{N}$, es decir, $\mathcal{N} \neq \emptyset$. Además, $\mathcal{N}$ es una familia finita ya que G sólo tiene una cantidad finita de subgrupos. Así, sea

$$\mathcal{N} = \{ S_1^*, S_2^*, ..., S_k^*\}.$$

Del teorema de Schreier-Zassenhaus [S-Z], S_1^* y S_2^* admiten un refinamiento, i.e., una serie normal que contiene a ambas, por tanto, existe una serie normal $S^* \in \mathcal{N}$ tal que S^* es un refinamiento de S_i^*, $1 \leq i \leq k$. Pero, $S^* \in \mathcal{N}$ implica que $\exists i \in \{1, 2, ..., k\}$ tal que $S^* = S_i^*$, por lo que, como $\cup_{j=1}^k \subset S^*$, se tiene que $S_i^* \subset \cup_{j=1}^k \subset S^* = S_i^*$, es decir, $S^* = \cup_{j=1}^k$. Sólo nos queda probar que S^* es maximal: Sea S'^* una serie normal de G tal que $S'^* \supset S^*$. Entonces $S'^* \in \mathcal{N}$ y claramente $S'^* \subset S^*$ de lo visto antes. Así, $S'^* = S^*$. ♣

Nota 11 En la resolución de este ejercicio hemos utilizado un razonamiento (proceso maximal) muy frecuente en demostraciones de existencia. En este caso, la cosa ha sido bastante sencilla dado que el conjunto total es finito, en caso de cardinalidad infinita se usa el llamado *Lema de Zorn*: "Si un conjunto ordenado es inductivo (todo subconjunto totalmente ordenado admite cota superior), entonces tiene algún elemento maximal".

Ex. 125 *Si G es un grupo finito, se define la longitud de G, $l(G)$, como el número de factores que tiene una serie de composición de G (notar que, del teorema de Jordan-Hölder, este número no depende de la serie de composición). Demostrar que, si H es un subgrupo normal de G, entonces se cumple*

$$l(G) = l(H) \cdot l(G/H) .$$

≡

Sean $l(H) = n$ y $l(G/H) = m$. Entonces existes series de composición

$$\{e\} = H_0 \preceq H_1 \preceq ... \preceq H_n = H \text{ en } H$$
$$\{H\} = N_0 \preceq N_1 \preceq ... \preceq N_m = G/H \text{ en } G/H.$$

Para cada $i = 1, 2, ..., m$, sea $G_i := \{x \in G \quad xH \in N_i\}$. Puede verse fácilmente que G_i cumple

1) G_i es un subgrupo de G que contiene a H.
2) G_i es un subgrupo normal de G_{i+1}.
3) $G_0 = H$ y $G_m = G$.

Así, se tiene que

$$\{e\} = H_0 \preceq H_1 \preceq ... \preceq H_n = H = G_0 \preceq G_1 \preceq ... \preceq G_m = G$$

es una serie normal de G. Puesto que dicha serie consta de $n+m$ factores, todo se reduce a ver que se trata de una serie de composición de G: Sea S^* la serie anterior y supongamos que $S'^* = \{T_0, T_1, ..., T_p\}$ es un refinamiento de S^*. Entonces $\exists q \leq p$ tal que $H = H_n = T_q$, y también $\{H_0, H_1, ..., H_n\} \subset \{T_0, T_1, ..., T_q\}$. Si llamamos S^*_H a esta serie, tenemos que S^*_H es un refinamiento de la serie $\{H_0, H_1, ..., H_n\}$ que es de composición en H, por tanto $q = n$ y $H_i = T_i$, $1 \leq 0 \leq n$. Además, puede verificarse sin dificultad que $\{T_n/H, T_{n+1}/H, ..., T_p/H\}$ es una serie normal de G/H que refina a $\{G_0/H, G_1/H, ..., G_m/H\} = \{N_0, N_1, ..., N_m\}$ que es una serie de composición de G/H; de ello deducimos que $p - n + 1 = m + 1$ y que $T_{i+n} = G_i$, $0 \leq i \leq m$. Ello demuestra que $S'^* = S^*$, como queríamos. ♣

Ex. 126 *Sea G un grupo abeliano de orden finito tal que $o(G) = p_1^{n_1} p_2^{n_2} \cdot ... \cdot p_m^{n_m}$, siendo $p_1, p_2, ..., p_m$ números primos distintos. Demostrar que*

$$l(G) \;=\; n_1 \,+\, n_2 \,+\, ... \,+\, n_m \;.$$

≡

Del T1S, existen $H_1, H_2, ..., H_m$ subgrupos de G tales que $o(H_i) = p_i^{n_i}$, $1 \leq i \leq m$. Al ser G abeliano y, como, para cada $i = 1, 2, ..., m$, se tiene que $H_i \cap (\prod_{j \neq i} H_j) = \{e\}$, podemos afirmar que $H_1 H_2 ... H_m$ es un subgrupo de G de orden $p_1^{n_1} p_2^{n_2} ... p_m^{n_m}$. Consecuentemente, $G = H_1 H_2 ... H_m$. Además, como todo grupo de orden potencia de primo admite una serie de composición con el número de factores que indica el exponente, tenemos que $l(H_i) = n_i$. Por tanto, todo se reduce a ver que $l(G) = l(H_1) + l(H_2) + ... + l(H_m)$:

Para ello basta con probar que, si $G = HK$, con $H \cap K = \{e\}$, entonces $l(G) = l(H) + l(K)$: Como $K \cong G/H$, utilizando el ejercicio anterior, $l(G) = l(H) + l(G/H) = l(H) + l(K)$. ♣

Ex. 127 *Hallar una serie de composición del grupo dihédrico D_6.*

≡

Sabemos de ejercicios anteriores en los que hablamos del grupo dihédrico que éste tiene la forma

$$D_6 \;=\; \{e, \rho, \rho^2, \rho^3, \rho^4, \rho^5, \sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma, \rho^4\sigma, \rho^5\sigma\},$$

con ρ indicando el giro de 60° y σ la simetría axial en un hexágono regular. Consideremos la serie

$$\{e\} \;\preceq\; \{e, \rho^3\} \;\preceq\; \langle\rho\rangle \;\preceq\; D_6.$$

Primero comprobamos que se trata de una serie normal: $\{e, \rho^3\}$ coincide con el centro de D_6, por lo que $\{e, \rho^3\}$ es un subgrupo normal de $\langle\rho\rangle$; además, para cada $i = 0, 1, 2, 3, 4, 5$, $\rho^i\sigma\langle\rho\rangle = \langle\rho\rangle\rho^i\sigma$, ya que, si $j = 0, 1, 2, 3, 4, 5$, entonces

$$(\rho^i\sigma)\rho^j \;=\; \rho^i(\sigma\rho^j) \;=\; \rho^i(\rho^{6-j}\sigma) \;=\; \rho^{i+6-j}\sigma \;=\; \rho^{6-j}(\rho^i\sigma),$$

de donde $\langle\rho\rangle$ es subgrupo normal de G. Finalmente, veamos que es una serie de composición: Si S^* es una serie normal que contiene a la nuestra, entonces tendríamos dos posibilidades

Una. Existe un subgrupo H en S^* tal que $\{e, \rho^3\} \preceq H \preceq \langle\rho\rangle$. Entonces, suponiendo que $H \neq \{e, \rho^3\}$, existe $i \in \{1, 2, 4, 5\}$ tal que $\rho^i \in H$. Ello implica que $H \supset \langle\rho^3, \rho^i\rangle$, pero es inmediato que $\langle\rho^3, \rho^i\rangle = \langle\rho\rangle$, i.e., $H = \langle\rho\rangle$. Es decir, H es un elemento de nuestra serie.
Dos. Existe un subgrupo H en S^* tal que $\langle\rho\rangle \preceq H \preceq D_6$. Ahora, suponiendo que $H \neq \langle\rho\rangle$, existe $i \in \{0, 1, 2, 3, 4, 5\}$ de modo que $\rho^i\sigma \in H$. Pero entonces $\sigma = \rho^{6-i}(\rho^i\sigma) \in H$, .lo que implica que $D_6 = \langle\rho, \sigma\rangle \subset H$. Es decir, $H = D_6$, por lo que pertenece a nuestra serie.

Hemos demostrado pues que nuestra serie es una serie normal maximal, o sea, una serie de composición en D_6. ♣

Nota 12 Otra forma, más elegante, de ver que la serie anterior es de composición en D_6 consiste en emplear el resultado teórico: " Una serie normal es de composición si y sólo si cada uno de sus cocientes es un grupo simple". Observar que:

$$o(\tfrac{\{e,\rho^3\}}{\{e\}}) = o(\{e, \rho^3\}) = 2$$
$$o(\tfrac{\langle\rho\rangle}{\{e,\rho^3\}}) = \tfrac{6}{2} = 3$$
$$o(\tfrac{D_6}{\langle\rho\rangle}) = \tfrac{12}{6} = 2,$$

por lo que, al tener orden primo, todos los grupos cocientes anteriores son grupos simples.

Ex. 128 *Demostrar que todo subgrupo de un grupo resoluble es resoluble.*

≡

Recordemos antes de todo que un grupo finito G se dice que es resoluble siempre que admite una serie de composición $\{e\} = H_0 \preceq H_1 \preceq ... \preceq H_n = G$ tal que cada uno de sus grupos cociente H_{i+1}/H_i es un grupo cíclico, $0 \leq i \leq n-1$. Conviene observar que la definición de grupo resoluble que aparece en muchos sitios es la siguiente: *Un grupo finito G se dice que es resoluble siempre que admite una serie normal de subgrupos $\{e\} = H_0 \preceq H_1 \preceq ... \preceq H_n = G$ tal que cada cociente H_{i+1}/H_i es abeliano.* Puede demostrarse que ambas definiciones son equivalentes. Mientras que la que usamos aquí es más cómoda (por su fortaleza) para ser aplicada cuando sepamos que el grupo es resoluble, la segunda definición es más útil para demostrar que un grupo es resoluble. Como consecuencia, es evidente que todo grupo finito abeliano es resoluble.

Antes de ponernos a resolver el ejercicio necesitamos el siguiente resultado auxiliar

Lema 3 *Sean H, F subgrupos de G tales que H es subgrupo normal de F y F/H es cíclico. Entonces, dado un subgrupo K cualquiera de G, se tiene que $(K \cap F)/(K \cap H)$ es cíclico.*

≡

Como $T := \{xH : x \in K \cap F\}$ es un subgrupo de F/H y éste es cíclico, se tiene que T también lo es. Por tanto, existe $x \in K \cap F$ tal que $T = \langle xH\rangle$. Todo consiste en ver que $(K \cap F)/(K \cap H) = \langle x(K \cap H)\rangle$:

$[\subset]$ $\forall y \in K \cap F$, como $yH \in T$, se tiene que $\exists n \in \mathbf{Z}$ tal que $yH = x^nH$. Así

$$y(K \cap H) = yK \cap yH = K \cap x^nH = x^nK \cap x^nH = x^n(K \cap H).$$

[$\supset$] $\forall n \in \mathbf{Z}$, $x^n \in K \cap F$ implica que $x^n(K \cap H) \in (K \cap F)/(K \cap H)$.

Volviendo al ejercicio, supongamos que G es resoluble y que $\{H_0, H_1, ..., H_n\}$ es una serie de composición de G tal que H_{i+1}/H_i es cíclico, $0 \leq i \leq n-1$. Sea T un subgrupo de G cualquiera. Para cada $i = 0, 1, ..., n$ podemos definir $T_i := T \cap H_i$ de modo que T_i es un subgrupo de T. Evitando la duplicdación de aquellos T_i que se repitan, es decir, los que cumplan que $T \cap H_i = T \cap H_{i+1}$, podemos formar una serie de composición de T

$$\{e\} = T'_0 \preceq T'_1 \preceq ... \preceq T'_m = T,$$

con $m \leq n$. Además, en virtud del lema previo tenemos que $T'_{i+1}/T'_i = (T \cap H_{i+1})/(T \cap H_i)$ es un grupo cíclico. ♣

Ex. 129 *Demostrar que si un grupo admite una serie normal tal que todos sus cocientes son resolubles, entonces el grupo es resoluble.*

≡

Sea G un grupo y sea $\{e\} = H_0 \preceq H_1 \preceq ... \preceq H_n = G$ tal que cada uno de sus grupos cociente H_{i+1}/H_i es un grupo resoluble, $0 \leq i \leq n-1$. Entonces, para cada $i = 0, 1, ..., n-1$, existe una serie de composición

$$\{H_i\} = T_{i0} \preceq T_{i1} \preceq ... \preceq T_{im_i} = H_{i+1}/H_i$$

de H_{i+1}/H_i tal que T_{ij+1}/T_{ij} es un grupo cíclico, $0 \leq j \leq m_i - 1$. Para cada $i = 0, 1, ..., n-1$ y cada $j = 0, 1, ..., m_i - 1$, sea

$$K_{ij} := \{ x \in G : xH_i \in T_{ij} \}.$$

De un problema anterior se deduce que $H_i = K_{i0} \preceq K_{i1} \preceq ... \preceq K_{im_i} = H_{i+1}$. Por tanto, el conjunto

$$\{ K_{ij} : 0 \leq i \leq n-1,\ 0 \leq j \leq m_i - 1 \}$$

es una serie normal de G. Además, $K_{ij+1}/K_{ij} \cong T_{ij+1}/T_{ij}$ es cíclico, $0 \leq i \leq n-1$, $0 \leq j \leq m_i - 1$. Así, podemos afirmar que G es un grupo resoluble. ♣

Ex. 130 *Demostrar que todo grupo de orden menor que* 60 *es resoluble.*

≡

Sea $o(G) < 60$. Sea $\{e\} = H_0 \preceq H_1 \preceq ... \preceq H_n = G$ una serie de composición de G. De la teoría correspondiente sabemos que H_{i+1}/H_i es un grupo simple, $0 \leq i \leq n-1$. Ahora bien, del Ex. 101, sabemos que todo grupo simple de orden menor que 60 es cíclico, por lo tanto, como $o(H_{i+1}/H_i) \leq o(G) < 60$, $0 \leq i \leq n-1$, se tiene que cada grupo cociente H_{i+1}/H_i es cíclico, por lo que G es resoluble. ♣

Ex. 131 *Demostrar que un producto directo de grupos resolubles es resoluble.*

≡

Hacemos la demostración para un producto directo de dos factores (para un número finito arbitrario de factores la demostración puede hacerse usando un argumento inductivo). Sean G y G' dos grupos resolubles. Antes necesitamos un lema auxiliar.

Lema 4 *Sea* $\{e\} = H_0 \preceq H_1 \preceq ... \preceq H_n = G$ *una serie normal de* G *cuyos cocientes son cíclicos. Entonces* G *es resoluble.*

$\equiv$ Fijémonos en que para que G sea resoluble ha de admitir una serie de composición de cocientes cíclicos, luego todo lo que hay que hacer es coger la serie normal anterior y refinarla hasta obtener una serie normal maximal de cocientes cíclicos. Supongamos que ya hemos formado la serie normal maximal (serie de composición) y que, por ejemplo, entre los factores H_i y H_{i+1} aparece un nuevo subgrupo H_i', es decir, tenemos

$$H_i \preceq H_i' \preceq H_{i+1}.$$

Entonces, como H_i'/H_i es subgrupo de H_{i+1}/H_i y éste es cílico, podemos afirmar que H_i'/H_i también es cíclico. Además, como todo cociente de un grupo cíclico lo sigue siendo y puesto que

$$H_{i+1}/H_i' \cong (H_{i+1}/H_i)/(H_i'/H_i),$$

deducimos que H_{i+1}/H_i' es cíclico. Lo que hemos visto para el nuevo factor H_i' vale para cualquier otro. Por tanto, la serie de composición formada sigue teniendo cocientes cíclicos y G es resoluble.

Volviendo a nuestro ejercicio, en virtud del lema anterior, todo se reduce a encontrar una serie normal del grupo producto $G \times G'$ que sea de cocientes cíclicos. Para ello, ya que G y G' son resolubles, partimos de dos series de composición de cocientes cíclicos

$$\{e\} = H_0 \preceq H_1 \preceq ... \preceq H_n \text{ en } G$$
$$\{e'\} = H_0' \preceq H_1' \preceq ... \preceq H_m' \text{ en } G'.$$

Suponiendo que $n \geq m$, consideremos la serie de subgrupos de $G \times G'$

$$\{(e,e')\} = H_0 \times H_0',\ H_1 \times H_1',\ ...,\ H_m \times H_m',\ H_{m+1} \times H_m',\ ...\ H_n \times H_m' = G \times G'.$$

Recordando que, si H y H' son subgrupos normales de G y de G', respectivamente, entonces $H \times H'$ es subgrupo normal de $G \times G'$, podemos afirmar que la serie anterior es una serie normal de $G \times G'$. Además, como también conviene recordar que, si G/H, y G'/H' son cíclicos también lo es $(G \times G')/(H \times H')$, tenemos que cada cociente de la serie normal anterior es un grupo cíclico, como queríamos. ♣

Ex. 132 *Sea* G *un grupo tal que para todo primo* p *divisor del orden de* G *hay exactamente un subgrupo* p*-Sylow. Demostrar que* G *es resoluble.*

$\equiv$

Sea $o(G) = p_1^{n_1}p_2^{n_2}...p_k^{n_k}$ la factorización del orden de G en factores primos. Para cada $i = 1, 2, ..., k$, sea H_i el único subgrupo p-Sylow de G. Sabemos de un ejercicio resuelto anteriormente que $G = H_1H_2...H_k$. Además, al tener orden potencia de primo, cada subgrupo H_i, $1 \leq i \leq k$, es resoluble. Del ejercicio previo, como G es isomorfo al producto directo $H_1 \times H_2 \times ... \times H_k$, se tiene que G es resoluble. ♣

1.9. El grupo simétrico

Ex. 133 *Demostrar que todo grupo es isomorfo a un subgrupo del grupo simétrico del conjunto soporte del grupo. [Teorema de Cayley]*

≡

Sea G un grupo cualquiera, de orden finito o infinito. Sea $\Sigma(G)$ el conjunto de todas las biyecciones de G en sí mismo. Sabemos que $\Sigma(G)$ posee estructura de grupo (en general no abeliano) para la composición de aplicaciones. Para demostrar el enunciado de este ejercicio, todo se reduce a establecer un homomorfismo de grupos inyectivo de G en $\Sigma(G)$. Para ello, definimos

$$\begin{array}{rccl} f & : & G & \longrightarrow & \Sigma(G) \\ & & x & \to & f(x): \ G \to G \\ & & & & \qquad\quad y \ \to f(x)(y) := xy. \end{array}$$

f bien definida: Para cada $x \in G$, veamos que $f(x) \in \Sigma(G)$, es decir, que $f(x)$ es biyectiva

$$\left.\begin{array}{l} f(x)(y) = f(x)(z) \ \to \ xy = xz \ \to \ y = z \ \to \ f \ inyectiva \\ \forall z \in G, \ tomando \ y := x^{-1}z \ \to \ f(x)(y) = xy = xx^{-1}z = z \ \to \ f \ sobre \end{array}\right\} \Rightarrow f \ biyectiva.$$

f homomorfismo: Para $x, y \in G$, veamos que $f(xy) = f(x) \circ f(y)$. Es decir, si $z \in G$

$$f(xy)(z) \ = \ (xy)z \ = \ x(yz) \ = \ x(f(y)(z)) \ = \ f(x)(f(y)(z)) \ = \ (f(x) \circ f(y))(z).$$

f inyectiva: Si $x \in Ker(f)$, entonces

$$Id_G \ = \ f(x) \ \to \ x \ = \ Id_G(x) \ = \ f(x)(x) \ = \ x^2 \ \to \ x = e.$$

Aplicando la descomposición canónica de un homomorfismo

$$G \ \cong \ G/Ker(f) \ \cong \ f(G) \ \equiv \ subgrupo \ de \ \Sigma(G). \ \clubsuit$$

Ex. 134 *En el grupo simétrico Σ_n, calcular el número de permutaciones que no dejan fijo elemento alguno del conjunto $N_n = \{1, 2, 3, ..., n\}$.*

≡

Para resolver este (desde nuestro punto de vista) interesante problema, hacemos uso del *Método de los Permanentes*, desarrollado en una conferencia impartida en el Centro Asociado de la UNED de Denia, el 2/4/82, por el insigne matemático (fallecido en Abril de 2014) D. Manuel Valdivia Ureña.

Un *permanente* de orden n es algo similar a un determinante del mismo orden, pero (más sencillo) para calcularlo no se realizan cambios de signo. Es decir

$$\left[\begin{array}{cc} a & b \\ c & d \end{array}\right] \ = \ ad + bc; \qquad \left[\begin{array}{cccc} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ..... & ..... & ..... & ..... \\ ..... & ..... & ..... & ..... \\ a_{n1} & a_{n2} & ... & a_{nn} \end{array}\right] \ = \ \sum_{\sigma \in \Sigma_n} a_{1\sigma_1} \cdot a_{2\sigma_2} \cdot ... \cdot a_{n\sigma_n}.$$

Un elemento $\sigma \in \Sigma_n$ se dice que es una permutación *anormal* siempre que, $\forall i \in N_n$, $\sigma_i \neq i$, es decir, cuando no deja fijo elemento alguno de N_n. Si llamamos A_n al conjunto de las permuationes anormales de Σ_n, lo que nos pide el ejercicio es que calculemos su cardinal, i.e., $card(A_n)$. Para ello, consideramos el siguiente permanente

$$P_n = \begin{bmatrix} 1-\delta_{11} & 1-\delta_{12} & \dots & 1-\delta_{1n} \\ 1-\delta_{21} & 1-\delta_{22} & \dots & 1-\delta_{2n} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 1-\delta_{n1} & 1-\delta_{n2} & \dots & 1-\delta_{nn} \end{bmatrix},$$

donde $\delta_{ij} = \left\{ \begin{array}{l} 1, \ si \ i = j, \\ 0, \ si \ i \neq j \end{array} \right\}$, es decir, δ_{ij} es la conocida *Delta de Kronecker*. Por tanto, el permanente P_n consta de 0's en la diagonal principal y de 1's en las restantes entradas. El valor de dicho permanente es

$$P_n = \sum_{\sigma \in \Sigma_n} a_{1\sigma_1} a_{2\sigma_2} \dots a_{n\sigma_n} = \sum_{\sigma \in A_n} a_{1\sigma_1} a_{2\sigma_2} \dots a_{n\sigma_n} + \sum_{\sigma \notin A_n} a_{1\sigma_1} a_{2\sigma_2} \dots a_{n\sigma_n}$$

$$= \sum_{\sigma \in A_n} a_{1\sigma_1} a_{2\sigma_2} \dots a_{n\sigma_n} = \sum_{\sigma \in A_n} 1 \cdot 1 \cdot \dots \cdot 1 = \sum_{\sigma \in A_n} 1 = card(A_n).$$

Así pues, todo se reduce a poder hallar el valor de P_n. Para ello, consideramos la función polinómica

$$f(x) = \begin{bmatrix} 1+x & 1 & \dots & 1 \\ 1 & 1+x & \dots & 1 \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1+x \end{bmatrix} = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \dots + a_n \cdot x^n .$$

Sabemos que los coeficientes $a_0, a_1, a_2, \dots, a_n$ se pueden calcular como

$$\begin{array}{rcl} a_0 & = & f(0) \\ a_1 & = & f'(0) \\ a_2 & = & \frac{f''(0)}{2!} \\ \dots & & \dots \\ \dots & & \dots \\ a_n & = & \frac{f^{(n)}(0)}{n!}. \end{array}$$

Pero, cómo se deriva un permanente? Muy fácil, todo consiste en una suma de n sumandos donde cada uno de los sumandos se obtiene derivando solamente una fila manteniendo las demás iguales. Así

$$f'(x) = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 1 & 1+x & \dots & 1 \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1+x \end{bmatrix} + \begin{bmatrix} 1+x & 1 & \dots & 1 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1+x \end{bmatrix}$$

$$+ \ldots + \begin{vmatrix} 1+x & 1 & \ldots & 1 \\ 1 & 1+x & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 \end{vmatrix} = n \cdot \begin{vmatrix} 1+x & 1 & \ldots & 1 \\ 1 & 1+x & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & \ldots & 1+x \end{vmatrix}_{(n-1)} .$$

$$f'(0) = n \cdot \begin{vmatrix} 1 & 1 & \ldots & 1 \\ 1 & 1 & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & \ldots & 1 \end{vmatrix}_{(n-1)} = n \cdot \sum_{\sigma \in \Sigma_{n-1}} 1 = n(n-1)! = n!$$

Para calcular $f''(x)$ y $f''(0)$ se procede análogamente derivando la expresión de $f'(x)$

$$f''(x) = n \left\{ \begin{vmatrix} 1 & 0 & \ldots & 0 \\ 1 & 1+x & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & \ldots & 1+x \end{vmatrix}_{(n-1)} + \begin{vmatrix} 1+x & 1 & \ldots & 1 \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & \ldots & 1+x \end{vmatrix}_{(n-1)} \right.$$

$$\left. + \ldots + \begin{vmatrix} 1+x & 1 & \ldots & 1 \\ 1 & 1+x & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 \end{vmatrix}_{(n-1)} \right\}$$

$$= n(n-1) \cdot \begin{vmatrix} 1+x & 1 & \ldots & 1 \\ 1 & 1+x & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & \ldots & 1+x \end{vmatrix}_{(n-2)} .$$

$$f'(0) = n(n-1) \begin{vmatrix} 1 & 1 & \ldots & 1 \\ 1 & 1 & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & \ldots & 1 \end{vmatrix}_{(n-2)} = n(n-1) \cdot \sum_{\sigma \in \Sigma_{n-2}} 1 = n(n-1)(n-2)! = n!$$

Así sucesivamente vemos que

$$f(0) = f'(0) = f''(0) = \ldots f^{(n)}(0) = n!$$

Consecuentemente

$$\left.\begin{array}{l} a_0 = \frac{n!}{0!} \\ a_1 = \frac{n!}{1!} \\ a_2 = \frac{n!}{2!} \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \\ a_n = \frac{n!}{n!} \end{array}\right\} \Rightarrow f(x) = n!\,(1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!}).$$

Finalmente

$$card(A_n) = P_n = f(-1) = n!\,[\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \ldots + \frac{(-1)^n}{n!}] = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \clubsuit$$

Nota 13 Observar, como cosa curiosa, que, para n muy grande, puesto que

$$\lim_{n\to\infty} \sum_{k=0}^{n} \frac{(-1)^k}{k!} = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} = \mathrm{e}^{-1} = \frac{1}{\mathrm{e}},$$

podemos concluir que el cociente entre el número de permutaciones anormales y el número de permutaciones totales es aproximadamente

$$\frac{card(A_n)}{card(\Sigma_n)} = \frac{n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!} \approx \frac{1}{e}.$$

Así es como Euler resolvió el llamado Problema de los encuentros, que dice así: " Si se tienen igual cantidad de cartas y de sobres numerados, cual es la probabilidad de que al meter cada carta en un sobre elegidos al azar sus números no coincidan nunca? "

Ex. 135 *En el grupo simétrico Σ_n, calcular el número de k-ciclos distintos.*

$\equiv$

Para $2 \leq k \leq n$, un k-ciclo en Σ_n es una permutación que se representa por $\gamma = (a_1, a_2, ..., a_k)$, donde $a_i \in N_n := \{1, 2, ..., n\}$, $1 \leq i \leq k$, que actúa del siguiente modo

$$\begin{array}{l} \gamma(a_1) = a_2 \\ \gamma(a_2) = a_3 \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \\ \gamma(a_k) = a_1 \\ \gamma(i) = i, \quad si\ i \in N_n \setminus \{a_1, a_2, ..., a_n\}. \end{array}$$

La cantidad de subconjuntos distintos de N_n con k elementos es $\binom{n}{k}$. Fijado un subconjunto de ellos $A := \{a_1, a_2, ..., a_k\}$, veamos cuántos k-ciclos distintos admite dicho subconjunto A. El conjunto A admite $k!$ permutaciones distintas, pero puede suceder

que dos permutaciones distintas de A determinen el mismo k-ciclo. Así, llamando Σ_A al conjunto de las permutaciones de A, establecemos la siguiente relación de equivalencia en Σ_A: Dadas $\sigma_1, \sigma_2 \in \Sigma_A$,

$$\sigma_1 \ eq \ \sigma_2 \quad \Leftrightarrow \quad \sigma_1 \text{ y } \sigma_2 \text{ generan el mismo ciclo.}$$

Observando el ejemplo:

$$(a_1, a_2, ..., a_k) \ eq \ (a_2, a_3, ..., a_1) \ eq \ ... \ eq \ (a_k, a_1, ..., a_{k-1}),$$

se ve que cada clase de equivalencia de esta relación consta de k elementos. Por tanto

$$\text{N° de k} - \text{ciclos generados por A} \ = \ \frac{card(\Sigma_A)}{k} \ = \ \frac{k!}{k} \ = \ (k-1)!$$

De donde

$$\text{N° de k} - \text{ciclos de } \Sigma_n \ = \ \binom{n}{k} \cdot (k-1)! \ = \ \frac{n!(k-1)!}{k!(n-k)!} \ = \ \frac{n(n-1)...(n-k+1)}{k}. \ \clubsuit$$

Ex. 136 *Demostrar que, para $n \geq 3$, dada una permutación $\sigma \in \Sigma_n$, $\sigma \neq e$ (donde e indica la permutación neutra, o sea, la identidad), existe una transposición $\beta \in \Sigma_n$ tal que $\sigma\beta \neq \beta\sigma$.*

≡

Recordemos que una transposición es una permutación $\beta \in \Sigma_n$ tal que deja a todos los elementos de N_n fijos excepto a dos $i \neq j$; entonces dicha traqnsposición se escribe como $\beta = (i, j)$ (observar que habríamos terminado antes diciendo que una transposición es simplemente un 2-ciclo). Sea $\sigma \in \Sigma_n$ tal que $\sigma \neq e$. Entonces existen $i, j \in N_n$, $i \neq j$, tales que $\sigma(i) = j$. Al ser $n \geq 3$, existe $k \in N_n \setminus \{i, j\}$. Sea $\beta = (k, j)$. Claramente

$$\left.\begin{array}{l} \sigma\beta(i) \ = \ \sigma(i) \ = \ j \\ \beta\sigma(i) \ = \ \beta(j) \ = \ k \end{array}\right\} \ \Rightarrow \quad \sigma\beta \ \neq \ \beta\sigma. \ \clubsuit$$

Nota 14 Observar que lo que hemos hecho en el ejercicio previo demuestra que el centro del grupo simétrico Σ_n, cuando $n \geq 3$, se reduce al elemento neutro, i.e.

$$Z_{\Sigma_n} \ = \ \{ \ e \ \}.$$

Ex. 137 *Demostrar que en Σ_n las permutaciones cíclicas disjuntas siempre conmutan.*

≡

Sean $\gamma = (a_1, a_2, ..., a_p)$ y $\delta = (b_1, b_2, ..., b_q)$ dos ciclos tales que $\{a_1, a_2, ..., a_p\} \cap \{b_1, b_2, ..., b_q\} = \emptyset$. Para verificar que $\gamma\delta = \delta\gamma$, dado $i \in N_n$, distinguimos tres posibilidades

Una. $i \notin \{a_1, a_2, ..., a_p, b_1, b_2, ..., b_q\}$. Entonces

$$\gamma\delta(i) \ = \ \gamma(i) \ = \ i \ = \ \delta(i) \ = \ \delta\gamma(i).$$

Dos. $i \in \{a_1, a_2, ..., a_p\}$. Ahora, suponiendo que $i = a_j$,

$$\left.\begin{array}{l} \gamma\delta(i) = \gamma(i) = \gamma(a_j) \\ \delta\gamma(i) = \delta\gamma(a_j) = \gamma(a_j) \text{ [pues } \gamma(\mathrm{a_j}) \in \{\mathrm{a_1}, ..., \mathrm{a_p}\}) \end{array}\right\} \Rightarrow \gamma\delta(i) = \delta\gamma(i).$$

Tres. $i \in \{b_1, b_2, ..., b_q\}$. Esta posibilidad es análoga a la Dos. ♣

Ex. 138 *En Σ_n, sea $0 \leq k \leq n$. Demostrar los siguientes apartados*

a) Si $n \neq 2k$, entonces Σ_n contiene al menos $\binom{n}{k}$ subgrupos isomorfos a $\Sigma_k \times \Sigma_{n-k}$, todos ellos conjugados.

b) Para $n = 4$, $k = 2$, verificar que no se cumple lo afirmado en el primer apartado.

≡

a) Sea $n \neq 2k$. Llamamos $P(n,k)$, y $F(n,k)$, a las familias de todos los subconjuntos de N_n con k elementos, y de todos los subgrupos de Σ_n que son isomorfos a $\Sigma_k \times \Sigma_{n-k}$, respectivamente. Definimos

$$\begin{array}{rccl} f & : & P(n,k) & \longrightarrow & F(n,k) \\ & & A & \to & f(A) := \{\, \sigma \in \Sigma_n \;:\; \sigma(A) = A\}, \end{array}$$

es decir, la imagen del subconjunto $A \subset N_n$ es el conjunto de todas la permutaciones que dejan invariante a A

f bien definida: Para $A \in P(n,k)$, hay que ver que $f(A)$ es un subgrupo de Σ_n isomorfo a $\Sigma_k \times \Sigma_{n-k}$. Es evidente que $f(A)$, por su definición, es el estabilizador de A para la actuación del grupo Σ_n sobre la familia de las partes del conjunto N_n. Por tanto, $f(A)$ es un subgrupo de Σ_n. Además, designanado por $\Sigma_A, \Sigma_{N_n \setminus A}$ a los grupos de permutaciones de los elementos de los conjuntos $A, N_n \setminus A$, respectivamente, está claro que $\Sigma_A \times \Sigma_{N_n \setminus A} \cong \Sigma_k \times \Sigma_{n-k}$, por lo que todo se reduce a establecer un isomorfismo de grupos entre $f(A)$ y $\Sigma_A \times \Sigma_{N_n \setminus A}$. Para ello, definimos

$$\begin{array}{rccl} g & : & f(A) & \longrightarrow & \Sigma_A \times \Sigma_{N_n \setminus A} \\ & & \sigma & \to & g(\sigma) = (\sigma_{|A}, \sigma_{|N_n \setminus A}). \end{array}$$

Como $\sigma \in f(A)$ garantiza que σ deja invariantes A y $N_n \setminus A$, es bastante fácil comprobar que g es isomorfismo. Luego $f(A) \in F(n,k)$.

f inyectiva: Sean $A, B \in P(n,k)$ tales que $f(A) = f(B)$, consideramos dos casos

1) $A \subset B$. Entonces $A = B$, ya que tienen el mismo cardinal k.

2) $A \not\subset B$. Sea $i \in A \setminus B$. Veamos que $A \cap B = \emptyset$: De no ser así, sea $j \in A \cap B$. Entonces

$$\left.\begin{array}{l} (i,j) \in f(A) \;\; [\text{pues (i,j)(A) = A}] \\ (i,j) \notin f(B) \; [\text{pues (i,j)(j) = i} \notin \text{B}] \end{array}\right\} \Rightarrow \text{Absurdo.}$$

Además, $A \cup B = N_n$, de lo contrario existe $j \in (N_n \setminus A) \cap (N_n \setminus B)$ y es fácil ver que $(i,j) \in f(B) \setminus f(A)$, otro absurdo. Hemos obtenido por tanto que

$$n = card(N_n) = card(A) + card(B) = 2k,$$

lo que contradice nuestra hipótesis de partida.

Así pues, el único caso posible es el primero, es decir, $A = B$. Como f es una inyección podemos asegurar que

$$card[F(n,k)] \geq card[P(n,k)] = \begin{pmatrix} n \\ k \end{pmatrix}.$$

Para ver que dichos subgrupos son conjugados entre sí, basta con demostrar que, llamando H al subgrupo imagen por f del conjunto $\{1,2,...,k\}$, i.e., $H = f(\{1,2,...,k\})$, entonces, dado $A = \{a_1, a_2, ..., a_k\} \in P(n,k)$, llamando $\{b_{k+1}, b_{k+2}, ..., b_n\}$ al conjunto $N_n \setminus A$, considerando la permutación

$$\begin{array}{l} \sigma(1) = a_1 \\ \sigma(2) = a_2 \\ ..... \\ ..... \\ \sigma(k) = a_k \\ \sigma(i) = b_i, \quad si\ i > k, \end{array}$$

obtenemos que $f(A) = \sigma H \sigma^{-1}$, ya que

$\forall \gamma \in f(A) \rightarrow \sigma^{-1}\gamma\sigma(\{1,2,...,k\}) = \sigma^{-1}\gamma(A) = \sigma^{-1}(A) = \{1,2,...,k\} \rightarrow \sigma^{-1}\gamma\sigma \in H \rightarrow \gamma \in \sigma H \sigma^{-1}$, y reciprocamente

$\forall \gamma \in H \rightarrow \sigma\gamma\sigma^{-1}(A) = \sigma\gamma(\{1,2,...,k\}) = \sigma(\{1,2,...,k\}) = A \rightarrow \sigma\gamma\sigma^{-1} \in f(A)$.

b) En Σ_4, para $k = 2$, veamos que sólo hay 4 subgrupos isomorfos a $\Sigma_2 \times \Sigma_2$, lo que prueba que la afirmación del apartado a) no es cierta cuando $n = 2k$, ya que $\begin{pmatrix} n \\ k \end{pmatrix} = 6 > 4$. Como $\Sigma_2 = \{e, \delta\}$, con $\delta = (1,2)$, tenemos que

$$\Sigma_2 \times \Sigma_2 = \{(e,e),(e,\delta),(\delta,e),(\delta,\delta)\} \text{ [el Viergruppe de Klein]}$$

Sea H un subgrupo de Σ_4 isomorfo a $\Sigma_2 \times \Sigma_2$. Como todo elemento de $H \setminus \{e\}$ tiene orden 2, podemos afirmar que todo elemento de $H \setminus \{e\}$ es o una transposición o un producto de transposiciones disjuntas. Ello implica que H sólo puede ser uno de los cuatro subgrupos siguientes

$$\begin{array}{l} H_1 = \{e, (12), (34), (12)(34)\} \\ H_2 = \{e, (13), (24), (13)(24)\} \\ H_3 = \{e, (14), (23), (14)(23)\} \\ H_4 = \{e, (12)(34), (13)(24), (14)(23)\}. \clubsuit \end{array}$$

Ex. 139 *En Σ_n, dada $\sigma \in \Sigma_n$, se define la forma de σ, que representamos por $Forma(\sigma)$, como la sucesión decreciente $o(\gamma_1) \geq o(\gamma_2) \geq ... \geq o(\gamma_k)$, donde $\gamma_1, \gamma_2, ..., \gamma_k$ son los únicos ciclos disjuntos tales que $\sigma = \gamma_1\gamma_2...\gamma_k$. Dados $\sigma, \tau \in \Sigma_n$, demotrar que σ y τ son conjugados si y sólo si $Forma(\sigma) = Forma(\tau)$.*

$\equiv$

[$\Leftarrow$] Sean $\sigma, \tau \in \Sigma_n$ tales que $Forma(\sigma) = Forma(\tau)$. Entonces existen $\gamma_1, \gamma_2, ..., \gamma_k$ ciclos disjuntos con $\sigma = \gamma_1\gamma_2...\gamma_k$ y existen $\delta_1, \delta_2, ..., \delta_p$ ciclos disjuntos con $\tau = \delta_1\delta_2...\delta_p$ de modo que

$$Forma(\sigma) = \{o(\gamma_1), o(\gamma_2), ..., o(\gamma_k)\} = \{o(\delta_1), o(\delta_2), ..., o(\delta_p)\} = Forma(\tau).$$

Claramente, $k = p$ y, para $i = 1, 2, ..., k$, $o(\gamma_i) = o(\delta_i) =: r_i$. Veamos que σ y τ son conjugados: Para verlo, supongamos que cada ciclo tiene la siguiente forma

$$\left\{ \begin{array}{l} \gamma_1 = (a_{11}, a_{12}, ..., a_{1r_1}) \\ \gamma_2 = (a_{21}, a_{22}, ..., a_{2r_2}) \\ ..... \\ ..... \\ \gamma_k = (a_{k1}, a_{k2}, ..., a_{kr_k}) \end{array} \right\}; \left\{ \begin{array}{l} \delta_1 = (b_{11}, b_{12}, ..., b_{1r_1}) \\ \delta_2 = (b_{21}, b_{22}, ..., b_{2r_2}) \\ ..... \\ ..... \\ \delta_k = (b_{k1}, b_{k2}, ..., b_{kr_k}) \end{array} \right\}.$$

Sea $\rho \in \Sigma_n$ tal que $\rho(a_{ij}) = b_{ij}$, $1 \leq i \leq k$, $1 \leq j \leq r_i$. Representando (como suele ser habitual en permutaciones)

$$\rho = \begin{pmatrix} a_{11}...a_{1r_1}a_{21}...a_{2r_2}...a_{k1}...a_{kr_k} \\ b_{11}...b_{1r_1}b_{21}...b_{2r_2}...b_{k1}...b_{kr_k} \end{pmatrix}, \text{ entonces : } \rho^{-1} = \begin{pmatrix} b_{11}...b_{1r_1}b_{21}...b_{2r_2}...b_{k1}...b_{kr_k} \\ a_{11}...a_{1r_1}a_{21}...a_{2r_2}...a_{k1}...a_{kr_k} \end{pmatrix}.$$

Así

$$\rho^{-1}\tau\rho = \begin{pmatrix} b_{11}...b_{1r_1}b_{21}...b_{2r_2}...b_{k1}...b_{kr_k} \\ a_{11}...a_{1r_1}a_{21}...a_{2r_2}...a_{k1}...a_{kr_k} \end{pmatrix} \cdot (b_{11}, b_{12}, ..., b_{1r_1})...(b_{k1}, b_{k2}, ..., b_{kr_k})$$

$$\cdot \begin{pmatrix} a_{11}...a_{1r_1}a_{21}...a_{2r_2}...a_{k1}...a_{kr_k} \\ b_{11}...b_{1r_1}b_{21}...b_{2r_2}...b_{k1}...b_{kr_k} \end{pmatrix}$$

$$= (a_{11}, a_{12}, ..., a_{1r_1})...(a_{k1}, a_{k2}, ..., a_{kr_k}) = \sigma.$$

[$\Rightarrow$] Sean $\sigma, \tau \in \Sigma_n$ tales que $\tau = \rho^{-1}\sigma\rho$, $\rho \in \Sigma_n$. Supongamos que la forma de σ es

$$Forma(\sigma) = \{o(\gamma_1), o(\gamma_2), ..., o(\gamma_k)\},$$

siendo

$$\begin{array}{l} \gamma_1 = (a_{11}, a_{12}, ..., a_{1r_1}) \\ \gamma_2 = (a_{21}, a_{22}, ..., a_{2r_2}) \\ ..... \\ ..... \\ \gamma_k = (a_{k1}, a_{k2}, ..., a_{kr_k}) \end{array}$$

ciclos disjuntos tales que $\sigma = \gamma_1\gamma_2...\gamma_k$. Consecuentemente, $Forma(\sigma) = \{r_1, r_2, ..., r_k\}$. Para cada $i = 1, 2, ..., k$ y cada $j = 1, 2, ..., r_i$, sea $b_{ij} := \rho^{-1}(a_{ij})$ y formemos los ciclos disjuntos

$$\begin{array}{l} \delta_1 = (b_{11}, b_{12}, ..., b_{1r_1}) \\ \delta_2 = (b_{21}, b_{22}, ..., b_{2r_2}) \\ ..... \\ ..... \\ \delta_k = (b_{k1}, b_{k2}, ..., b_{kr_k}). \end{array}$$

Entonces

$$\tau = \rho^{-1}\sigma\rho = \rho^{-1}(a_{11}, a_{12}, ..., a_{1r_1})...(a_{k1}, a_{k2}, ..., a_{kr_k})\rho$$
$$= (b_{11}, b_{12}, ..., b_{1r_1})...(b_{k1}, b_{k2}, ..., b_{kr_k}) = \delta_1\delta_2...\delta_k,$$

de donde

$$Fotma(\tau) = \{o(\delta_1), o(\delta_2), ..., o(\delta_p)\} = \{r_1, r_2, ..., r_k\} = Forma(\sigma). \clubsuit$$

Ex. 140 *Calcular el número de elementos de* Σ_n *cuya forma es* $\{r_1, r_2, ..., r_k\}$.

$\equiv$

Sea N el número que se pide. Como hay que formar k ciclos disjuntos de órdenes $r_1 \geq r_2 \geq ... \geq r_k$, está claro que

$$\left.\begin{array}{l} \text{Posibles } r_1 - \text{ciclos de } N_n: \quad \left(\begin{array}{c} n \\ r_1 \end{array}\right) \cdot (r_1 - 1)! \\ \text{Posibles } r_2 - \text{ciclos de } N_n \setminus \{r_1 \textit{ elementos}\}: \quad \left(\begin{array}{c} n - r_1 \\ r_2 \end{array}\right) \cdot (r_2 - 1)! \\ ..... \\ ..... \\ \text{Posibles } r_k - \text{ciclos de } N_n \setminus \{r_1 + ... + r_{k-1} \textit{ elementos}\}: \quad \left(\begin{array}{c} n - r_1 - ... - r_{k-1} \\ r_k \end{array}\right) \cdot (r_k - 1)! \end{array}\right\}$$

$$\Rightarrow N = \left(\begin{array}{c} n \\ r_1 \end{array}\right) \cdot (r_1 - 1)! \cdot \left(\begin{array}{c} n - r_1 \\ r_2 \end{array}\right) \cdot (r_2 - 1)!... \left(\begin{array}{c} n - r_1 - ... - r_{k-1} \\ r_k \end{array}\right) \cdot (r_k - 1)!. \clubsuit$$

Ex. 141 *Demostrar que* Σ_n *está generado por las transposiciones* $(1,2); (2,3); ...; (n-1, n)$, *i.e.,*

$$\Sigma_n = \langle\ (1,2); (2,3); ...; (n-1, n)\ \rangle.$$

$\equiv$

Sabemos que todo elemento de Σ_n se puede expresar como producto de transposiciones. Por tanto

$$\Sigma_n = \langle\ \{(i,j) : i < j\}\ \rangle.$$

Así pues, todo se reduce a ver que cualquier transposición (i,j), $i < j$, está generada por $(1,2); (2,3); ...; (n-1, n)$. Evidente

$$(i,j) = (j-1, j)(j-2, j-1)...((i+1, i+2)...(i, i+1)...(j-2, j-1)(j-1, j). \clubsuit$$

Nota 15 En aras de comprender mejor lo hecho arriba, considerar un ejemplo concreto: En Σ_n, $n \geq 4$,

$$(2,4) = (3,4)(2,3)(3,4).$$

Ex. 142 *Demostrar que*

$$\Sigma_n = \langle\ (1,2); (1,2,...,n)\ \rangle.$$

$\equiv$

Del ejercicio anterior sabemos que $\Sigma_n = \langle (1,2);(2,3);...;(n-1,n) \rangle$, por tanto todo consiste en ver que

$$(i,i+1) \in \langle (1,2);(1,2,...,n) \rangle, \quad 1 \leq i < n.$$

Lo vemos poco a poco

$$\begin{array}{l} (1,2) = (1,2) \\ (2,3) = (1,2,...,n)(1,2)(1,2,...,n)^{-1} \\ (3,4) = (1,2,...,n)(2,3)(1,2,...,n)^{-1} = (1,2,...,n)^2(1,2)(1,2,...,n)^{-2} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (n-1,n) = (1,2,...,n)^{n-1}(1,2)(1,2,...,n)^{-n+1}. \clubsuit \end{array}$$

Ex. 143 *Se define el signo de una permutación $\sigma \in \Sigma_n$ como $sig(\sigma) = (-1)^k$, siendo k el número de transposiciones en que se factoriza σ. Determinar el signo de un ciclo.*

$\equiv$

Sea $\gamma = (a_1, a_2, ..., a_k)$ un k-ciclo. Claramente

$$\gamma = (a_1, a_2, ..., a_k) = (a_1, a_2)(a_2, a_3)...(a_{k-1}, a_k) \Rightarrow signo(\gamma) = (-1)^{k-1}. \clubsuit$$

Ex. 144 *En Σ_n, se define el grupo alternado A_n como el subgrupo de Σ_n formado por todas las permutaciones de signo positivo, i.e.*

$$A_n = \{ \sigma \in \Sigma_n : signo(\sigma) = 1 \}.$$

Demostrar que el grupo alternado A_n está generado r los 3-ciclos $(1,i,n)$, $1 \leq i \leq n-1$.

$\equiv$

Es un resultado conocido que todo elemento de A_n se puede expresar como producto de 3-ciclos. Así pues, todo se reduce a ver que, si γ es un ciclo de la forma $\gamma = (j,h,k)$, $j \neq h \neq k \in N_n$, entonces γ se puede expresar como producto de 3-ciclos de la forma $(1,i,n)$. Consideramos tres posibilidades

1) $\{j,h,k\} \cap \{1,n\} = \emptyset$. Entonces

$$\gamma = (j,h,k) = (1,j,n)(1,h,n)(1,k,n)(1,j,n)(1,h,n).$$

2) $\{j,h,k\} \cap \{1,n\} \neq \emptyset$. Aquí consideramos tres subcasos

(2.1) $j \in \{1,n\}$.

$$j=1 \rightarrow \begin{cases} n \notin \{h,k\} \rightarrow \gamma = (j,h,k) = (1,h,k) = (1,k,n)^2(1,h,n) \\ n \in \{h,k\} \rightarrow \begin{cases} n=h \rightarrow \gamma = (j,h,k) = (1,n,k) = (1,k,n)^{-1} \\ n=k \rightarrow \gamma = (j,h,k) = (1,h,n) \end{cases} \end{cases}$$

$$j=n \rightarrow \begin{cases} 1 \notin \{h,k\} \rightarrow \gamma = (j,h,k) = (n,h,k) = (1,k,n)^2(1,h,n)(1,k,n) \\ 1 \in \{h,k\} \rightarrow \begin{cases} 1=h \rightarrow \gamma = (j,h,k) = (n,1,k) = (1,k,n) \\ 1=k \rightarrow \gamma = (j,h,k) = (n,h,1) = (1,h,n)^{-1} \end{cases} \end{cases}$$

(2.2) $h \in \{1,n\}$. Análogo al subcaso anterior.

(2.3) $k \in \{1,n\}$. Análogo al subcaso anterior. $\clubsuit$

Ex. 145 *En* Σ_4

a) Demostrar que $H = \{e, (12)(34), (13)(24), (14)(23)\}$ *es un subgrupo normal de* A_4.

b) Demostrar que $K = \{e, (12)(34)\}$ *es subgrupo normal de* H, *pero no lo es de* A_4.

≡

Fijemos las transposiciones $t_1 := (12)$, $t_2 := (13)$, $t_3 := (14)$, $t_4 := (23)$, $t_5 := (24)$, $t_6 := (34)$ y sean

$$\alpha := t_1t_6, \quad \beta := t_2t_5, \quad \gamma := t_3t_4.$$

a) Claramente, como $signo(\alpha) = signo(\beta) = signo(\gamma) = 1$, se tiene que $H = \{e, \alpha, \beta, \gamma\} \subset A_4$. A continuación demostramos algo más fuerte que lo pedido, de hecho vamos a ver que H es subgrupo normal de todo Σ_4: Para ello, puesto que todo elemento de $\Sigma_4 = \langle t_1, t_2, t_3, t_4, t_5, t_6 \rangle$, todo consiste en comprobar que, para $1 \leq i \leq 6$, $t_iH = Ht_i$, lo que claramente ilustra el cuadro siguiente

	t_1	t_2	t_3	t_4	t_5	t_6
α	$t_1\alpha$	$t_2\gamma$	$t_3\beta$	$t_4\beta$	$t_5\gamma$	$t_6\alpha$
β	$t_1\gamma$	$t_2\beta$	$t_3\alpha$	$t_4\alpha$	$t_5\beta$	$t_6\gamma$
γ	$t_1\beta$	$t_2\alpha$	$t_3\gamma$	$t_4\gamma$	$t_5\alpha$	$t_6\beta$.

b) Como H es abeliano, está claro que K es subgrupo normal de H (observar primero que $K \subset H$). Sin embargo $t_1t_2 \in A_4$, ya que $signo(t_1t_3) = (-1)^2 = 1$, y

$$\left.\begin{array}{rcl} t_1t_2\ K & = & \{t_1t_2,\ t_1t_2\alpha\} \\ K\ t_1t_2 & = & \{t_1t_2,\ \alpha t_1t_2\} = \{t_1t_2,\ t_1t_2\gamma\} \end{array}\right\} \Rightarrow t_1t_2\ K \neq K\ t_1t_2 \Rightarrow K \not\trianglelefteq A_4. \clubsuit$$

Ex. 146 *Demostrar que* A_4 *no tiene subgrupos de orden* 6.

≡

Supongamos que H es un subgrupo de A_4 tal que $o(H) = 6$. Entonces

$$[A_4 : H] = \frac{o(A_4)}{o(H)} = \frac{12}{6} = 2 \Rightarrow H \trianglelefteq A_4.$$

Del teorema de Cauchy, ya que $o(H) = 2 \cdot 3$, existe un subgrupo K de H tal que $o(K) = 3$. Entonces K es un grupo cíclico, por lo que $\exists \gamma \in K$ tal que $K = \langle\ \gamma\ \rangle$. Sea $\gamma = (a, b, c)$, $a \neq b \neq c \in \{1, 2, 3, 4\}$. Sea ahora $\alpha = (i, j, k)$ un 3-ciclo arbitrario. Consideramos la permutación β tal que

$$\beta(a) = i, \quad \beta(b) = j, \quad \beta(c) = k.$$

Entonces se tiene que $\beta \in A_4$, pues $signo(\beta) = signo(\gamma) = 1$. Pero

$$\alpha = (i, j, k) = \beta\gamma\beta^{-1} \in \beta\ H\ \beta^{-1} = H,$$

lo que implica que H contiene todos los 3-ciclos. Como es bien sabido que A_4 está generado por los 3-ciclos, tenemos que $H = A_4$, lo que es absurdo. ♣

Nota 16 El ejercicio anterior proporciona un ejemplo de grupo $(A_4, o(A_4) = 12)$ tal que, para cierto divisor (obviamente no primo) de su orden $(6|12)$ no admite subgrupos de orden dicho divisor.

Ex. 147 *Construir series de composición de* Σ_2, Σ_3 *y* Σ_4, *demostrando que son grupos resolubles.*

$\equiv$

$\Sigma_2 = \{e, (12)\} \Rightarrow \{e\} \preceq \Sigma_2$ es una serie de composición de Σ_2. Como $\Sigma/\{e\} \cong \Sigma_2 = \langle\ (12)\ \rangle$, dicho cociente es cíclico y Σ_2 es resoluble.

$\Sigma_3 = \{e, (12), (13), (23), (123)(132)\} \Rightarrow \{e\} \preceq H := \{e, (123), (132)\} \preceq \Sigma_3$ es una serie de composición de Σ_3. Como $H = \langle\ (123)\ \rangle$, se tiene que $H/\{e\}$ es cíclico y también lo es Σ_3/H, ya que $o(\Sigma/H) = [\Sigma : H] = \frac{6}{3} = 2$.

$$\Sigma_4 = \{e, (12), (13), (14), (23), (24), (34), (123), (124), (132), (134), (142), (143), (234), (243), (1234), (1243), (1324), (1342), (1423), (1432), (12)(34), (13)(24), (14)(23)\}$$

$$\{e\} \preceq H_1 := \{e, (12)(34)\} \preceq H_2 := \{e, (12)(34), (13)(24), (14)(23)\} \preceq A_4 \preceq \Sigma_3$$

es una serie de composición de Σ_4, ya que

H_1 es subgrupo normal de H_2, pues H_2 (de nuevo el Viergruppe) es abeliano,
H_2 es subgrupo normal de A_4, como vimos anteriormente,
A_4 es subgrupo normal de Σ_4, (en general, $\mathrm{A_n} \preceq \Sigma_\mathrm{n}$).

Además

$$\left.\begin{array}{l} o(H_1/\{e\}) = 2 \rightarrow H_1/\{e\} \text{ cíclico} \\ o(H_2/H_1) = 2 \rightarrow H_2/H_1 \text{ cíclico} \\ o(A_4/H_2) = 3 \rightarrow A_4/H_2 \text{ cíclico} \end{array}\right\} \Rightarrow \Sigma_4 \text{ es resoluble. } \clubsuit$$

Ex. 148 *Demostrar que, para* $n > 4$, *el único subgrupo propio normal de* Σ_n *es* A_n.

$\equiv$

Sea H un subgrupo normal de Σ_n distinto de $\{e\}$ y de Σ_n. Entonces $H \cap A_n$ es un subgrupo normal de A_n y, como $n \geq 5$ implica que A_n es simple, tenemos dos posibilidades
Una. $H \cap A_n = \{e\}$. Sea $\sigma \in H$; entonces, si $\alpha \in \Sigma_n$, $\alpha\sigma\alpha^{-1}\sigma^{-1} \in H \cap A_n$, pues $\alpha\sigma\alpha^{-1} \in \alpha H\alpha^{-1} = H$ y $signo(\alpha\sigma\alpha^{-1}\sigma^{-1}) = signo(\alpha)^2 \cdot signo(\sigma)^2 = 1$. Por tanto $\alpha\sigma\alpha^{-1}\sigma^{-1} = e$ y $\alpha\sigma = \sigma\alpha$. Ello significa que $\sigma \in Z_{\Sigma_n} = \{e\}$, lo que es absurdo.
Dos. $H \cap A_n = A_n$. Entonces $A_n \subset H$. Para ver que $H = A_n$, razonando por reducción al absurdo, supongamos que $H \not\subset A_n$. Sea pues $\sigma \in H \setminus A_n$. Entonces $signo(\sigma) = -1$, de donde $\sigma = t_1 t_2 ... t_{2p+1}$, con t_i, $1 \leq i \leq 2p+1$, siendo transposiciones y supongamos que $t_{2p+1} = (a, b)$. Observar que

$$(a, b) = t_{2p+1} = (t_1 t_2 ... t_{2p})^{-1}\sigma \in A_n H = H.$$

Sea ahora $i, j)$ una transposición cualquiera. Tomando $\alpha \in \Sigma_n$ tal que $\alpha(a) = i$, $\alpha(b) = j$, tenemos que

$$(i,j) \;=\; \alpha\ (a,b)\ \alpha^{-1} \;=\; \alpha\ t_{2p+1}\ \alpha^{-1} \;\in\; \alpha\ H\ \alpha^{-1} \;=\; H.$$

Hemos demostrado que H contiene a cualquier transposición de Σ_n, de lo que, como Σ_n está generado por las transposiciones, deducimos que $H = \Sigma_n$, lo que contradice nuestra hipótesis inicial. ♣

Ex. 149 *Para $n > 4$, sea $y = f(x_1, x_2, ..., x_n)$ una función de n variables reales. Designemos por N al número de funciones distintas que se obtienen al permutar las n variables. Demostrar que, si $N > 2$, entonces $N \geq n$.*

≡

Consideremos la actuación del grupo simétrico Σ_n sobre el conjunto $\mathbf{R}^{\mathbf{R}^n}$ dada por

$$\begin{array}{lll} * : & \Sigma_n \times \mathbf{R}^{\mathbf{R}^n} & \longrightarrow \mathbf{R}^{\mathbf{R}^n} \\ & (\sigma, g) & \to \sigma * g \ : \mathbf{R}^n \to \mathbf{R} \\ & & (x_1, x_2, ..., x_n) \to (\sigma * g)(x_1, x_2, ..., x_n) = g(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}) \end{array}$$

Entonces el valor de N coincide con el cardinal de la órbita de f bajo la actuación descrita antes. Es decir

$$N \;=\; card(\Sigma_n * f) \;=\; [\Sigma_n : est(f)].$$

Si $N > 2$, entonces $[\Sigma_n : est(f)] > 2$ implica que $est(f) \neq A_n$. Como, para $n > 4$, A_n es el único subgrupo propio de Σ_n de índice menor que n, deducimos claramente que $N = [\Sigma_n : est(f)] \geq n$. ♣

Ex. 150 *En un barco hay tres cuerdas, la 1, la 2 y la 3, que penden verticalmente y que están cruzadas por cierto número de cuerdas horizontales de manera que cada cuerda horizontal une solamente dos cuerdas verticales, la 1 con la 2, o la 2 con la 3. Suponiendo que tres marineros se deslizan hacia abajo cada uno por una de las tres cuerdas verticales con la condición de que al tropezar con una cuerda horizontal cruzante han de cruzarla y cambiar de cuerda vertical, demostrar que al llegar abajo los marineros se hallan siempre en cuerdas verticales distintas.*

≡

Se trata de un ejercicio de aplicación de la teoría del grupo simétrico. En particular, estamos en Σ_3 y supongamos que $\{x_1, x_2, x_3\}$ representa a los tres marineros. Dada $\sigma \in \Sigma_3$, al escribir

$$\sigma * (x_1, x_2, x_3) \;=\; (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$$

significamos que el marinero $x_{\sigma(1)}$ se encuentra en la cuerda vertical 1, el marinero $x_{\sigma(2)}$ se encuentra en la cuerda vertical 2 y que el marinero $x_{\sigma(3)}$ se encuentra en la cuerda vertical 3. Llamando t_1, t_2 a las transposiciones $(1,2), (2,3)$, respectivamente, es decir,

$t_1 * (x_1, x_2, x_3) = (x_2, x_1, x_3)$ y $t_2 * (x_1, x_2, x_3) = (x_1, x_3, x_2)$, la bajada de cuerdas de los tres marineros se reduce a calcular, suponiendo que hay k cuerdas horizontales,

$$(\sigma_1\sigma_2...\sigma_k) * (x_1, x_2, x_3), \quad \sigma_1, \sigma_2..., \sigma_k \in \{t_1, t_2\}.$$

Llamando $\gamma := \sigma_1\sigma_2...\sigma_k$, queda claro que

$$(\sigma_1\sigma_2...\sigma_k) * (x_1, x_2, x_3) = \gamma * (x_1, x_2, x_3) = (x_{\gamma(1)}, x_{\gamma(2)}, x_{\gamma(3)}),$$

de donde, como γ es una aplicación biyectiva de $\{1, 2, 3\}$ en sí mismo, es evidente que $\gamma(1), \gamma(2), \gamma(3)$ son distintos. ♣

Capítulo 2

Teoría de cuerpos

En todo este capítulo F hará referencia a un cuerpo, y por cuerpo entendemos un cuerpo conmutativo.

2.1. Generalidades y ejemplos de cuerpos

Ex. 151 *Demostrar*

a) $\forall a \in F,\ 0 \cdot a = 0.$

b) $\forall a \in F,\ (-1) \cdot a = -a.$

$\equiv$

a)

$$0 \cdot a + a = 0 \cdot a + 1 \cdot a = (0+1) \cdot a = 1 \cdot a = a \Rightarrow 0 \cdot a = 0.$$

b)

$$(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1+1) \cdot a = 0 \cdot a = 0 \Rightarrow (-1) \cdot a = -a. \clubsuit$$

Ex. 152 *Demostrar que, si* $a, b \in F$ *son tales que* $a \cdot b = 0$, *entonces* $a = 0$, *ó,* $b = 0$.

$\equiv$

Suponiendo que $a \neq 0$, como $F^* = F \setminus \{0\}$ es un grupo multiplicativo y $a \in F^*$, existe $a^{-1} \in F^*$. Entonces

$$0 = a^{-1} \cdot 0 = a^{-1}ab = 1 \cdot b = b. \clubsuit$$

Ex. 153 *Si* $a, b \in F$, $b \neq 0$, *usamos la notación* $\frac{a}{b}$ *para indicar* $a \cdot b^{-1}$. *Demostrar*

a) $\forall a, b \in F^*,\ \frac{1}{\frac{a}{b}} = \frac{b}{a}.$

b) $\forall a, b, c, d \in F,\ b \neq 0,\ d \neq 0,\ \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}.$

$\equiv$

Vamos a usar el que $\frac{x}{y} = \frac{z}{u}$ si y sólo si $xu = yz$, ya que

$$\frac{x}{y} = \frac{z}{u} \Leftrightarrow xy^{-1} = zu^{-1} \Leftrightarrow x = zu^{-1}y = zyu^{-1} \Leftrightarrow xu = yz.$$

a)

$$\frac{a}{b} \cdot \frac{b}{a} = (ab^{-1})(ba^{-1}) = (ab^{-1})(ab^{-1})^{-1} = 1.$$

b)

$$(\frac{a}{b} + \frac{c}{d}) \cdot bd = (ab^{-1} + cd^{-1}) \cdot bd = ad + bc. \clubsuit$$

Ex. 154 *Construir un cuerpo de* 4 *elementos.*

≡

Si F ha de ser un cuerpo de cardinal 4, está claro que va ser de la forma $F = \{0, 1, x, y\}$. Vamos a definir las operaciones "suma" y "producto"de modo que F sea en efecto un cuerpo. Lo hacemos en los siguientes diagramas de Cayley

$+$	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

;

$\cdot$	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	1
y	0	y	1	x

Observar que $(F, +)$ es el Viergruppe y que $(F^*, \cdot)$ es un grupo cíclico, ya que $F^* = \langle\, x \,\rangle$. Para ver que $(F, +, \cdot)$ es un cuerpo sólo hay que demostrar que se cumple la propiedad distributiva, es decir, si $a, b, c \in F$, entonces $a(b + c) = ab + ac$. Para verlo fabricamos un árbol de casos

$a = 0, ó\ b = 0, ó\ c = 0 \rightarrow\ 0 = 0 + 0, ó,\ ac = ac, ó,\ ab = ab$
$a = 1 \rightarrow\ a(b + c) = b + c = ab + ac$
$b = c \rightarrow\ a(b + c) = a(b + b)0a \cdot 0 = 0 = ab + ab = ab + ac$
$a = x,\ b \neq c,\ b \neq 0,\ c \neq 0 \rightarrow$ $\begin{cases} x(1 + x) = xy = 1 = x + y = x \cdot 1 + xx \\ x(1 + y) = xx = y = x + 1 = x \cdot 1 + xy \\ x(x + y) = x \cdot 1 = x = y + 1 = xx + xy \end{cases}$
$a = y,\ b \neq c,\ b \neq 0,\ c \neq 0 \rightarrow$ Análogo al caso anterior $\clubsuit$

Ex. 155 *Dado un cuerpo F, en $F \times F$ definimos:*

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Determinar las condiciones que ha de cumplir F para que $F \times F$ con las operaciones definidas se un cuerpo.

$\equiv$

Veamos que: $F \times F$ es cuerpo $\Leftrightarrow \forall (a,b) \in F \times F \setminus \{(0,0)\}, \quad a^2 + b^2 \neq 0$.

[$\Rightarrow$] El cero de $F \times F$ es claramente $(0,0)$. Por tanto, al tener que $F \times F$ es cuerpo, como $F \times F \setminus \{(0,0)\}$ es un grupo multiplicativo, se tiene que, para $(a,b) \in F \times F \setminus \{(0,0)\}$, tenemos lo siguiente

$$\left.\begin{array}{l}(a,b),(b,a) \in F \times F \setminus \{(0,0)\} \ \rightarrow \ (a,b)\cdot(b,a) \in F \times F \setminus \{(0,0)\} \\ (a,b)\cdot(b,a) \ = \ (ab-ba, a^2+b^2) \ = \ (0, a^2+b^2)\end{array}\right\}$$

$$\Rightarrow \quad (0, a^2+b^2) \ \neq \ (0,0).$$

Ello implica que $a^2 + b^2 \neq 0$.

[$\Leftarrow$] Es inmediato comprobar que $F \times F$ es un grupo abeliano para la suma definida. Además la multiplicación definida es asociativa, tiene unidad $(1,0)$, es conmutativa y es distributiva. Así, para que $F \times F$ sea cuerpo sólo resta verificar dos cosas: Que $\cdot$ es estable en $F \times F \setminus \{(0,0)\}$, y que todo elemento de $F \times F \setminus \{(0,0)\}$ tiene inverso.

Para ver lo primero, sean $(a,b),(c,d) \in F \times F \setminus \{(0,0)\}$. Queremos ver que $(ac - bd, ad + bc) \neq (0,0)$. Llamando $x := ac - bd$, $y := ad + bc$, tenemos

$$\begin{array}{rcl} ax + by & = & (a^2+b^2)c \\ bx - ay & = & -(a^2+b^2)d \\ cx + dy & = & (c^2+d^2)a \\ dx - cy & = & -(c^2+d^2)b. \end{array}$$

Así, en el caso de que $x = y = 0$, a partir de las igualdades anteriores se tendría, ya que partimos de la hipótesis de que $a^2 + b^2 \neq 0$, $c^2 + d^2 \neq 0$, que: $a = b = c = d = 0$, lo que es absurdo.

Para ver la segunda cosa, sea $(a.b) \in F \times F \setminus \{(0,0)\}$. Todo se reduce a comprobar que $(a(a^2+b^2)^{-1}, -b(a^2+b^2)^{-1})$, que claramente pertenece a $F \times F \setminus \{(0,0)\}$, es el inverso de (a,b):

$$(a,b)\cdot(a(a^2+b^2)^{-1}, -b(a^2+b^2)^{-1}) = (a^2(a^2+b^2)^{-1}+b^2(a^2+b^2)^{-1}, -ab(a^2+b^2)^{-1}+ba(a^2+b^2)^{-1})$$

$$= (1,0). \ \clubsuit$$

Ex. 156 *Demostrar que:*

a) Todo homomorfismo de cuerpos no nulo es inyectivo,

b) Todo homomorfismo de cuerpos suprayectivo es un isomorfismo.

$\equiv$

a) Sea $f : E \rightarrow F$ un homomorfismo entre los cuerpos E, F tal que $f \neq 0$. Si $Ker(f) \neq \{0\}$, entonces $\exists x \neq 0, \quad x \in Ker(f)$. Pero

$$\forall y \in E, \quad f(y) \ = \ f(xx^{-1}y) \ = \ f(x)f(x^{-1}y) \ = \ 0 \cdot f(x^{-1}y) \ = \ 0.$$

Ello significa que $f = 0$, lo que es absurdo.

b) Si $f : E \to F$ es un homomorfismo sobre, como $f(E) = F$ y $card(F) \geq 2$ (si $0 = 1 \to \forall y \in F,\ y = y \cdot 1 = y \cdot 0 = 0 \to F = \{0\}$. De hecho en la definición de cuerpo se exige que 0 y 1 sean distintos). Por tanto, f no es el homomorfismo nulo y, aplicando el apartado anterior, se tiene que f es inyectiva, es decir, f es un isomorfismo de cuerpos♣

Ex. 157 *Sea E un cuerpo y $F \subset E$. Demostrar que F es un subcuerpo de E si y sólo si se cumplen*

1) $F^* \neq \emptyset$.

2) $\forall a, b \in F,\ a - b \in F$.

3) $\forall a, b \in F, b \neq 0,\ \frac{a}{b} \in F$.

≡

[$\Rightarrow$] Si F es subcuerpo de E, entonces $(F, +)$ y $(F^*, \cdot)$ son subgrupos de $(E, +)$ y de $(E^*, \cdot)$, respetivamente. Ello implica que

$$F^* \neq \emptyset$$
$$\forall a, b \in F \to \begin{cases} a - b \in F \\ si\ a \neq 0,\ b \neq 0 \to \frac{a}{b} = ab^{-1} \in F^* \end{cases}$$

[$\Leftarrow$] De la condición 2) se sigue que $(F, +)$ es subgrupo de $(E, +)$. Como $F^* \neq \emptyset$, de lacondición 3) se tiene que $(F^*, \cdot)$ es un subgrupo de $(E^*, \cdot)$. Consecuentemente $(F, +, \cdot)$ es un subcuerpo de E. ♣

Ex. 158 *Un cuerpo numérico (también llamado campo numérico, ya que en inglés la palabra cuerpo es "field", que se traduce por " campo") es cualquier subcuerpo de* $\mathbf{C}$*, el cuerpo de los números complejos con la adición y multiplicación complejas. Si* $\mathbf{Q}(\sqrt{2}) = \{\ a + b\sqrt{2}\ :\ a, b \in \mathbf{Q}\ \}$*, demostrar que* $\mathbf{Q}(\sqrt{2})$ *es un cuerpo numérico.*

≡

Como tenemos que ver que $\mathbf{Q}(\sqrt{2})$ es subcuerpo de $\mathbf{C}$, aplicando el ejercicio anterior, hay que verificar el cumplimiento de las tres condiciones allí indicadas.

1) $\mathbf{Q}(\sqrt{2})^* \neq \emptyset$.

2) $\forall a + b\sqrt{2}, c + d\sqrt{2} \in \mathbf{Q}(\sqrt{2})$

$$a + b\sqrt{2} - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in \mathbf{Q}(\sqrt{2}.$$

3) $\forall a + b\sqrt{2}, c + d\sqrt{2} \in \mathbf{Q}(\sqrt{2}),\ c + d\sqrt{2} \neq 0$

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}.$$

La última expresión corresponde a un elemento de $\mathbf{Q}(\sqrt{2})$, ya que $c^2 - 2d^2 \neq 0$, de lo contrario

$$c^2 = 2d^2 \to 2 = (\frac{c}{d})^2 \to \sqrt{2} \in \{\pm\frac{c}{d}\} \subset \mathbf{Q}.$$ Absurdo ♣

Ex. 159 *Demostrar que todo cuerpo numérico contiene a* $\mathbf{Q}$.

$\equiv$

Sea F un cuerpo numérico, es decir, F es un subcuerpo de $\mathbf{C}$. Por definición de cuerpo $0, 1 \in F$. Entonces

$$\{0, \pm 1\} \subset F \rightarrow \forall n \in \mathbf{N}, \left\{ \begin{array}{l} n = 1 + 1 + \overset{(n)}{\cdots} + 1 \rightarrow n \in F \\ -n = (-1) + (-1) + \overset{(n)}{\cdots} + (-1) \rightarrow -n \in F \end{array} \right\} \Rightarrow \mathbf{Z} \subset F.$$

Finalmente, si $r \in \mathbf{Q}$, por definición de número racional, existen $a, b \in \mathbf{Z}$, $b \neq 0$ tales que $r = \frac{a}{b} = ab^{-1}$. Así, como $a \in \mathbf{Z} \subset F$ y $b \in \mathbf{Z} \subset F \rightarrow b^{-1} \in F$, se deduce que $r = ab^{-1} \in F$. ♣

Ex. 160 *Dado un cuerpo F, se define su característica, $carac(F)$, como*

$$carac(F) := \left\{ \begin{array}{l} \text{mín}\{n \in \mathbf{N} : \exists a \in F^* / \ na = 0\}, \quad \text{si este conjunto es no vacio,} \\ 0, \quad \text{en caso contrario} \end{array} \right.$$

Demostrar que, si $carac(F) = n$, entonces:

a) $\forall a \in F^*, \quad na = 0.$

b) n *es primo.*

$\equiv$

a) $carac(f) = n$ implica la existencia de cierto elemento $x \in F^*$ tal que $nx = 0$. Entonces

$$\forall a \in F^*, \quad na = nxx^{-1}a = 0 \cdot (x^{-1}a) = 0.$$

b) Sea $x \in F^*$ tal que $nx = 0$. Entonces, suponiendo que $n = pq$, $p, q \in \mathbf{N}$,

$$0 = nx = pqx \rightarrow \left\{ \begin{array}{l} qx = 0 \rightarrow n = car(F) \leq q \leq n \rightarrow q = n \\ qx \neq 0 \rightarrow qx \in F^* \rightarrow n = car(F) \leq p \leq n \rightarrow p = n. \end{array} \right. ♣$$

Ex. 161 *Demostrar:*

a) $carac(F) = 0$ *si y sólo si existe un homomorfismo de cuerpos inyectivo de* $\mathbf{Q}$ *en* F.

b) $carac(F) = p$ *si y sólo si entonces existe un homomorfismo de cuerpos inyectivo de* $\mathbf{Z}_p$ *en* F.

$\equiv$

a)

$[\Rightarrow]$ Suponiendo que $carac(F) = 0$, dados $n, m \in \mathbf{Z}$, llamamos $\hat{n}, \hat{m}$ a los elementos de F dados por $n \cdot 1, m \cdot 1$, respectivamente. Así, definimos

$$\begin{array}{rcl} f : \mathbf{Q} & \longrightarrow & F \\ \frac{n}{m} & \rightarrow & f(\frac{n}{m}) = \hat{n} \cdot \hat{m}^{-1}. \end{array}$$

f bien definida: Si $m \neq 0$, es obvio que $\hat{m} = m \cdot 1 \neq 0$, i.e. $\hat{m} \in F^*$, por que existe $\hat{m}^{-1} \in F$. f homomorfismo de cuerpos: Dados $\frac{n}{m}, \frac{p}{q} \in \mathbf{Q}$

$$\left. \begin{array}{l} f(\frac{n}{m} + \frac{p}{q}) = f(\frac{nq+mp}{mq}) = \widehat{(nq + mp)} \cdot (\widehat{mq})^{-1} = [(nq + mp) \cdot 1] \cdot [(mq) \cdot 1]^{-1} \\ f(\frac{n}{m}) + f(\frac{p}{q}) = \hat{n}\hat{m}^{-1} + \hat{p}\hat{q}^{-1} = [(n \cdot 1)(m \cdot 1)^{-1}] + [(p \cdot 1)(q \cdot 1)^{-1}] \end{array} \right\} \Rightarrow$$

$$[(n\cdot 1)(m\cdot 1)^{-1}+(p\cdot 1)(q\cdot 1)^{-1}](mq\cdot 1)=(n\cdot 1)(q\cdot 1)+(m\cdot 1)(p\cdot 1)=(nq+mp)\cdot 1$$
$$\Rightarrow\ [(nq+mp)\cdot 1]\cdot[(mq)\cdot 1]^{-1}=[(n\cdot 1)(m\cdot 1)^{-1}]+[(p\cdot 1)(q\cdot 1)^{-1}].$$

Además

$$f(\frac{n}{m}\cdot\frac{p}{q})=f(\frac{np}{mq})=(np\cdot 1)(mq\cdot 1)^{-1}=(n\cdot 1)(p\cdot 1)(m\cdot 1)^{-1}(q\cdot 1)^{-1}=f(\frac{n}{m})f(\frac{p}{q}).$$

f inyectivo: Si $f(\frac{n}{m})=0$, entonces

$$0\ =\ f(\frac{n}{m})\ =\ (n\cdot 1)(m\cdot 1)^{-1}\ \Rightarrow\ n\cdot 1=0\ \overset{car(F)=0}{\Rightarrow}\ n=0\ \Rightarrow\ \frac{n}{m}=0.$$

[$\Leftarrow$] Suponiendo que existe un homomorfismo inyectivo $f:\mathbf{Q}\to F$, razonando por reducción al absurdo, supongamos que $carac(F)\neq 0$. Por definición, ello supone la existencia de $n\in\mathbf{N}$, $a\in F^*$ tales que $na=0$. Al ser f inyectivo, $f(n)\in F^*$ y también $nf(n)=f(n^2)\in F^*$. Pero

$$n\cdot f(n)\ =\ naa^{-1}f(n)\ =\ 0\cdot a^{-1}f(n)\ =\ 0.\ \text{Absurdo.}$$

b) [$\Rightarrow$] Suponiendo que $carac(F)=p$, definimoa

$$\begin{array}{rccl} f & : & Z_p & \longrightarrow & F \\ & & \overline{k} & \to & f(\overline{k})=k\cdot 1. \end{array}$$

f bien definida: Si $k,n\in\mathbf{Z}$ son tales que $\overline{k}=\overline{n}$, entonces existe $m\in\mathbf{Z}$ tal que $k-n=mp$. Por tanto, $k\cdot 1-n\cdot 1=mp\cdot 1=0$, de donde $f(\overline{k})=k\cdot 1=n\cdot 1=f(\overline{n})$.
f homomorfismo de cuerpos: Dadas $\overline{k},\overline{n}\in\mathbf{Z}_p$

$$\begin{array}{l} f(\overline{k}+\overline{n})\ =\ f(\overline{k+n})\ =\ (k+n)\cdot 1\ =\ k\cdot 1+n\cdot 1\ =\ f(\overline{k})+f(\overline{n}) \\ f(\overline{k}\cdot\overline{n})=f(\overline{kn})=(kn)\cdot 1=k\cdot(n\cdot 1)=[(n\cdot 1)\cdot 1]\overset{(k)}{\cdots}[(n\cdot 1)\cdot 1] \\ =(k\cdot 1)\cdot(n\cdot 1)=f(\overline{k})\cdot f(\overline{n}). \end{array}$$

f inyectivo: Sea $\overline{k}\in Ker(f)$. Entonces $0=f(\overline{k})=k\cdot 1$. Suponiendo que $k\geq 0$, lo que no supone pérdida alguna de generalidad, y utilizando la división entera: $\exists c,r\in\mathbf{N}\cup\{0\}$ tales que $k=cp+r$, $0\leq r<p$. Así

$$0\ =\ k\cdot 1\ =\ (cp+r)\cdot 1\ =\ cp\cdot 1+r\cdot 1\ =\ 0+r\cdot 1\ =\ r\cdot 1\ \overset{(definicion\ de\ carac.)}{\Rightarrow}\ r=0$$
$$\Rightarrow\ k=cp\ \Rightarrow\ \overline{k}=\overline{0}.$$

[$\Leftarrow$] Suponiendo que existe un homomorfismo f inyectivo entre los cuerpos $\mathbf{Z}_p$ y F (por cierto, no creo haberlo dicho, para que $\mathbf{Z}_p$ sea cuerpo p ha de ser primo, como así se requiere para ser característica), como $f(\overline{1})=1\in F^*$, se tiene que $p\cdot f(\overline{1})=p\cdot 1=f(\overline{p})=f(\overline{0})=0$. Además, si $k\in\mathbf{N}$ es tal que $k\cdot f(\overline{1})=0$, entonces $f(\overline{k})=0$ y $\overline{k}=\overline{0}$, lo que implica que $p\mid k$, i.e., $k\geq p$. Hemos demostrado que p es el menor entero positivo tal que $p\cdot f(1)=0$, es decir, $carac(F)=p$. ♣

Ex. 162 *Sea* $carac(F) = p > 0$. *Demostrar:*

a) La aplicación $\varphi : F \to F$ *tal que* $\varphi(a) = a^p$, $a \in F$, *es un homomorfismo.*

b) Si F *es finito, entonces* φ *es un isomorfismo.*

$\equiv$

a) Dados $a, b \in F$

$$\varphi(a+b) = (a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + ... + \binom{p}{p-1} ab^{p-1} + b^p = (*)$$

Veamos que, para $k = 1, 2, ..., p-1$, $\binom{p}{k}$ es múltiplo de p:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = p\,[\frac{(p-1)...(p-k+1)}{k!}] \in \mathbf{N},$$

ello implica que el cociente $\frac{(p-1)...(p-k+1)}{k!} \in \mathbf{N}$, ya que p es primo y $k < p$. Así, como $car(F) = p$, en $(*)$ todos los sumandos son 0 excepto los extremos, o sea

$$(*) = a^p + b^p = \varphi(a) + \varphi(b).$$

Además

$$\varphi(ab) = (ab)^p = (ab)\overset{(p)}{...}(ab) = a^p b^p = \varphi(a)\varphi(b).$$

b) Suponiendo que F es un cuerpo finito, todo se reduce a ver que φ es una aplicación inyectiva. Para ello, al ser homomorfismo, sea $a \in Ker(\varphi)$. Entonces, suponiendo que $a \neq 0$,

$$0 = \varphi(a) = a^p \overset{(mult.por\, a^{-1})}{\to} 0 = a^{p-1} \to 0 = a^{p-2}.... a = 0. \text{ Absurdo. } \clubsuit$$

Ex. 163 *Sea* E *un espacio vectorial sobre el cuerpo* F. *Sea* S *un subconjunto no vacío de* E. *Consideramos el conjunto*

$$V = \{v \in E : v \text{ es combinación lineal de S}\}.$$

Demostrar que V *es un espacio vectorial sobre* F.

$\equiv$

Se supone al lector conocedor de la teoría de los espacios vectoriales correspondiente al Algebra Lineal. Así pues, lo que pide el ejercicio es que demostremos que V es un subespacio vectorial de E. Análogamente a como sucede en el Algebra Lineal, donde se habla de espacios vectoriales reales o complejos, cuando el espacio está definido sobre un cuerpo arbitrario F también puede demostrarse fácilmente la validez del teorema de caracterización de los subespacios vectoriales. Por lo tanto, todo consiste en ver que, si $a, b \in F$ y $u, v \in V$, entonces $au + bv \in V$. Veámoslo: Por definición del conjunto V, existen $c_1, ...c_p, d_1, ..., d_q \in F$ y $u_1, ..., u_p, v_1, ..., v_q \in S$ de modo que

$$\left.\begin{array}{l} u = c_1u_1 + ... + c_pu_p \\ v = d_1v_1 + ... + d_qv_q \end{array}\right\} \Rightarrow au + bv = a\sum_{i=1}^{p} c_iu_i + b\sum_{j=1}^{q} d_jv_j$$

$$= ac_1u_1 + ... + ac_pu_p + bd_1v_1 + ... + bd_qv_q \in V. \clubsuit$$

Ex. 164 *Si E es un espacio vectorial sobre el cuerpo F, se llama dimensión de E sobre F y se representa como $[E:F]$ al menor cardinal δ tal que exista un subconjunto de vectores de E linealmente independientes que es generador de E (lo que se dice usualmente, una base) y que posee cardinal δ. Cuando δ es un cardinal finito, se dice que el espacio E es de dimensión finita. Demostrar que si E es un espacio vectorial sobre F tal que tiene dimensión finita, entonces cualquier subespacio suyo V también es de dimensión finita y se cumple que $[V:F] \leq [E:F]$.*

≡

Demostramos ambas cosas en una. Supongamos que $[E:F] = n$. Por tanto, existe una base de E de la forma $B = \{u_1, u_2, ..., u_n\}$. Supongamos que V tiene dimensión mayor que n. Entonces existe B_V, con $card(B_V) > n$, formado por vectores de V que son linealmente independientes. Sea $v_1 \in B_V$. Sabemos que, para ciertos $a_1, a_2, ..., a_n \in F$, $v_1 = a_1v_1 + a_2v_2 + ... + a_nv_n$. Suponiendo (comodidad) que $a_1 \neq 0$, se obtiene que u_1 es C.L. del sistema $\{v_1, u_2, ..., u_n\}$. Cogemos ahora $v_2 \in B_V \setminus \{v_1\}$, análogamente se obtiene que, como v_2 es inicialmente C.L. de $\{u_1, u_2, ..., u_n\}$, v_2 es C.L. de $\{v_1, u_2, ..., u_n\}$. Suponiendo que $v_2 = b_1v_1 + b_2u_2 + ... + b_nu_n$ y que $b_2 \neq 0$ (alguno de los $b_2, ..., b_n$ ha de ser no nulo, de lo contario v_1, v_2 serían L.D.), obtenemos que u_2 es C.L. de $\{v_1, v_2, u_3, ..., u_n\}$. Repitiendo este proceso exactamente n veces obtenemos que $u_1, u_2, ...u_n$ son C.L. de $\{v_1, v_2, ..., v_n\}$. Finalmente, como $card(B_V) > n$, tomando $v_{n+1} \in B_V \setminus \{v_1, ..., v_n\}$, se tiene que v_{n+1} es C.L. inicialemente de $\{u_1, u_2, ..., u_n\}$ y por lo tanto es C.L. de $\{v_1, v_2, ..., v_n\}$. Ello es absurdo, ya que los vectores de B_V son L.I. ♣

Ex. 165 *Sea V un subespacio vectorial del espacio vectorial E sobre el cuerpo F. En E se define la relación binaria: $u \sim v \leftrightarrow u - v \in V$. Demostrar:*

a) $\sim$ es una relación de equivalencia, llamada congruencia vectorial (módulo V).

b) El conjunto cociente $E/\sim$, que se representa generalmente como E/V, admite una estructura de espacio vectorial sobre F.

c) Si $[E:F] < \infty$, entonces $[E/V:F] < \infty$

≡

a) Veamos que $\sim$ cumple las tres propiedades que definen a las relaciones de equivalencia:
Reflexiva: $\forall u \in E$, como $u - u = \vec{0} \in V$, obviamente $u \sim u$.
Simétrica: Si $u, v \in E$, son tales que $u \sim v$, entonces

$$\left.\begin{array}{l} u - v \in V \\ v - u = -(u - v) \in V \end{array}\right\} \Rightarrow v \sim u.$$

Transitiva: Si $u, v, w \in E$, son tales que $u \sim v$, $v \sim w$, entonces

$$\left.\begin{array}{l} u \sim v \rightarrow u - v \in V \\ v \sim w \rightarrow v - w \in V \end{array}\right\} \Rightarrow u - w = (u - v) + (v - w) \in V \Rightarrow u \sim w.$$

b) Para poder tener una estructura de espacio vectorial sobre el cuerpo F en el conjunto cociente E/V, se necesitan dos operaciones que han de cumplir una serie de propiedades.

La primera operación (la suma vectorial) es una operación en E/V que ha de dotar a dicho conjunto de estructura de grupo abeliano. Vamos a definirla: Conforme suele ser habitual en las estructuras algebraicas cociente las operaciones entre clases de equivalencia suelen definirse a partir de las operaciones entre los representantes de dichas clases, es decir, resumiendo,

$$\text{clase "operación" clase} \;=\; \text{clase[representante "operación" representante]}.$$

Así, dadas dos clases $u+V, v+V$ de E/V (se representan así, ya que:
$\overline{u} = \{x \in E : x \sim u\} = \{x \in E : x-u \in V\} = \{x \in E : x = u+(x-u) \in u+V\} = u+V$), definimos

$(u+V) + (v+V) \;=\; (u+v)+V$. [i.e., la suma de clases es igual a la clase de la suma]

$+$ bien definida en E/V: Tenemos que verificar que la definicón de esta suma de clases no depende del representante elegido. Así, supongamos que $u \sim u', v \sim v'$, tenemos que ver que $(u+V)+(v+V) = (u'+V)+(v'+V)$, es decir, que $(u+v)+V = (u'+v')+V$, o sea, que $(u+v) \sim (u'+v')$:

$$\left.\begin{array}{l} u \sim u' \;\to\; u-u' \in V \\ v \sim v' \;\to\; v-v' \in V \end{array}\right\} \Rightarrow (u+v) \;-\; (u'+v') \;=\; (u-u') \;+\; (v-v') \;\in\; V$$

$$\Rightarrow (u+v) \sim (u'+v').$$

Para ver que $(E/V, +)$ es un grupo abeliano, verificamos el cumplimiento de las cinco cosas:
Estable: Si $u+V, v+V \in E/V$, entonces $(u+V)+(v+V) = (u+v)+V \in E/V$.
Asociativa: Si $u+V, v+V, w+V \in E/V$, entonces
$((u+V)+(v+V))+(w+V) \;=\; ((u+v)+V)+(w+V) \;=\; ((u+v)+w)+V \;=\; (u+(v+w))+V \;=\; (u+V)+((v+w)+V) \;=\; (u+V)+((v+V)+(w+V))$.
Neutro: Si $u+V \in E/V$, entonces $(u+V)+(0+V) \;=\; (u+0)+V \;=\; u+V$, lo que indica que $0+V$, que se escribe V, es el elemento neutro de $(E/V, +)$.
Simétricos: Si $u+V \in E/V$, entonces $(u+V)+(-u+V) = (u+(-u))+V = 0+V = V$, lo que indica que el elemento simétrico para esta operación de $u+V$ es $-u+V$, o sea, $-(u+V) = -u+V$.
Conmutativa: Si $u+V, v+V \in E/V$, entonces $(u+v)+(v+V) = (u+v)+V = (v+u)+V = (v+V)+(u+V)$, ya que, al ser E espacio vectorial, $(E,+)$ es un grupo abeliano.

La segunda operación es la que usualmente recibe el nombre de ley externa. Es decir, es una operación que "multiplica" escalares (elementos del cuerpo F) por vectores (elementos de E/V) para dar vectores. Así definimos, para $a \in F$, $u+V \in E/V$, $a(u+v) := au+V$. Como siempre que se trabaje con espacios cociente, primero hay que ver que la operación definida no depende del representante de las clases.
Ley externa bien definida: Sean $u, u' \in E$ tales que $u \sim u'$. Entonces, dado $a \in F$, queremos ver que $a(u+V) = a(u'+V)$, es decir, que $au+V = au'+V$, o sea, que

$au \sim au'$; para ello

$$\left.\begin{array}{l} u \sim u' \rightarrow\ u - u' \in V \\ au - au' = a(u-u') \in V \text{ (V es subespacio)} \end{array}\right\} \Rightarrow\ au \sim au'.$$

Finalmente, nos queda verificar el cumplimiento de los llamados 4 Axiomas.
Axioma I: [Distributiva de escalares respecto de vectores] Si $a \in F$, $u+V, v+V \in E/F$,

$$a[(u+V)+(v+V)] = a[(u+v)+V] = a(u+v)+V = (au+av)+V$$

$$= (au+V)+(av+V) = a(u+V)+a(v+V).$$

Axioma II: [Distributiva de vectores respecto de escalares] Si $a, b \in F$, $u+V \in E/F$,

$$(a+b)(u+V) = ((a+b)u)+V = (au+bu)+V = (au+V)+(bu+V) = a(u+V)+b(u+V).$$

Axioma III: [Asociativa mixta (como la paella)] Si $a, b \in F$, $u+V \in E/F$,

$$a[b(u+V)] = a(bu+V) = a(bu)+V = ((ab)u)+V = (ab)(u+V).$$

Axioma IV: [Escalar unidad] Si $u+V \in E/F$, entonces la unidad $1 \in F$ cumple que

$$1(u+V) = (1 \cdot u)+V = u+V.$$

c) Supongamos que $[E : F] = n$. De un ejercicio anterior, sabemos que si llamamos $m := [V : F]$, entonces $m \leq n$. Sea $B_V = \{v_1, v_2, ..., v_m\}$ una base de V. Ampliamos B_V hasta formar una base de todo E de la forma

$$B \ = \ \{\ v_1, v_2, ..., v_m, v_{m+1}, v_{m+2}, ..., v_n\ \}.$$

Todo ahora se reduce a probar que el sistema de E/V dado por $B_{E/V} = \{v_{m+1}+V, v_{m+2}+V, ..., v_n+V\}$ es una base de E/V. Para ello, primero veamos que dichos vectores de E/V son linealmente independientes: Sean $a_1, a_2, ..., a_{n-m} \in F$ tales que $a_1(v_{m+1}+V) + a_2(v_{m+2}+V) + ... + a_{n-m}(v_n+V) = 0+V = V$. Entonces

$$V \ = \ \sum_{i=1}^{n-m} a_i(v_{m+i}+V) \ = \ (\sum_{i=1}^{n-m} a_i v_{m+i}) + V \ \Rightarrow \ \sum_{i=1}^{n-m} a_i v_{m+i} \in V,$$

lo que implica la existencia de escalares $b_1, b_2, ..., b_m \in F$ tales que

$$\sum_{i=1}^{n-m} a_i v_{m+i} \ = \ \sum_{j=1}^{m} b_j v_j \ \Rightarrow \ \sum_{j=1}^{m} b_j v_j \ - \ \sum_{i=1}^{n-m} a_i v_{m+i} \ = \vec{0}\ .$$

Ello implica, ya que todos los vectores involucrados en la igualdad anterior son L.I. por estar en B, que todos los escalares que aparecen son nulos, en particular

$$a_1 \ = \ a_2 \ = \ ... \ a_{n-m} = \ 0.$$

Veamos seguidamente que los vectores de $B_{E/V}$ generan al espacio E/V: Dado $u + V \in E/V$, como $u \in E$, y B es base de E, existen escalars $a_1, a_2, ..., a_n \in F$ tales que $u = a_1v_1 + a_2v_2 + ... + a_nv_n$. Entonces

$$u+V = (\sum_{i=1}^{n} a_iv_i)+V = \sum_{i=1}^{n}(a_iv_i+V) = \sum_{i=1}^{m}(a_iv_i+V) + \sum_{j=m+1}^{n}(a_jv_j+V)$$

$$= V + \sum_{j=m+1}^{n}(a_jv_j+V) = \sum_{j=m+1}^{n} a_j(v_j+V). \clubsuit$$

Nota 17 Notar que hemos demostrado la siguiente igualdad importante en espacios vectoriales de dimensión finita

$$[E/V : F] = [E : F] - [V : F] .$$

Ex. 166 *Demostrar que* $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$ *y que* $[\mathbf{C} : \mathbf{R}] = 2$.

≡

Recordemos que $\mathbf{Q}(\sqrt{2})$ es el subcuerpo de $\mathbf{R}$ formado por todas los números reales de la forma $a + b\sqrt{2}$, con $a, b \in \mathbf{Q}$. Para demostrar que $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$ no hay más que obtener una base de $\mathbf{Q}(\sqrt{2})$ que tenga cardinal 2. Así pues, veamos que $\{1, \sqrt{2}\}$ es base de $\mathbf{Q}(\sqrt{2})$.

$$\left.\begin{array}{l} 0 = a\cdot 1 + b\sqrt{2}, a, b \in \mathbf{Q} \rightarrow \ a = b = 0 \rightarrow \{1, \sqrt{2}\} \ L.I. \\ a + b\sqrt{2} = a\cdot 1 + b\sqrt{2} \rightarrow \{1, \sqrt{2}\} \ S.G. \end{array}\right\} \Rightarrow \{1, \sqrt{2}\} \text{ es base de } \mathbf{Q}(\sqrt{2}).$$

Análogamente a lo hecho con $\mathbf{Q}(\sqrt{2})$, para ver que $[\mathbf{C} : \mathbf{R}] = 2$ hay que encontrar una base de $\mathbf{C}$ de cardinal 2. De hecho, como $\mathbf{C} = \{a + b\mathbf{i} \ : \ a, b \in \mathbf{R}\}$, procediendo similarmente a lo hecho antes, se demuestra que $\{1, \mathbf{i}\}$ es una base de $\mathbf{C}$ sobre $\mathbf{R}$. $\clubsuit$

Ex. 167 *Sea* $\omega := e^{\frac{2\pi\mathbf{i}}{3}}$. *Sea* $\mathbf{Q}(\omega) = \{a + b\omega \ : \ a, b \in \mathbf{Q}\}$. *Demostrar que* $\mathbf{Q}(\omega)$ *es una extensión de* $\mathbf{Q}$ *y que* $[\mathbf{Q}(\omega) : \mathbf{Q}] = 2$.

≡

Veamos primero que $\mathbf{Q}(\omega)$ es un subcuerpo de $\mathbf{C}$, es decir, que se trata de un cuerpo numérico. Si $a + b\omega, c + d\omega \in \mathbf{Q}(\omega)$, entonces, puesto que $\omega = \frac{-1}{2} + \mathbf{i}\frac{\sqrt{3}}{2}$,

$$\left.\begin{array}{l} (a+b\omega)-(c+d\omega) = (a-c)+(b-d)\omega \in \mathbf{Q}(\omega) \\ \frac{a+b\omega}{c+d\omega} = \frac{(a+b\omega)(c-d\omega)}{(c+d\omega)(c-d\omega)} = (\frac{ac+bd-ad}{c^2+d^2-cd}) + (\frac{bc-ad}{c^2+d^2-cd})\ (\frac{-1}{2} + \mathbf{i}\frac{\sqrt{3}}{2}) \in \mathbf{Q}(\omega) \end{array}\right\}$$

$$\Rightarrow \ \mathbf{Q}(\omega) \text{ es subcuerpo de } \mathbf{C}.$$

Además, como, si $a \in \mathbf{Q}$, entonces $a = a + 0\cdot\omega$, se tiene que $a \in \mathbf{Q}(\omega)$, es decir, $\mathbf{Q} \subset \mathbf{Q}(\omega)$, por lo que $\mathbf{Q}(\omega)$ es un cuerpo extensión del cuerpo $\mathbf{Q}$. De modo similar a lo hecho en el ejercicio anterior, se ve que $\{1, \omega\}$ es una base de $\mathbf{Q}(\omega)$ sobre $\mathbf{Q}$, luego $[\mathbf{Q}(\omega) : \mathbf{Q}] = 2$. $\clubsuit$

Nota 18 Cuando un cuerpo E es extensión de otro F, se demuestra que E posee estructura de espacio vectorial sobre F, por lo que tiene sentido hablar de $[E : F]$. Es decir, el valor $[E : F]$ es la dimensión de E sobre F.

Ex. 168 *Sea F un cuerpo finito tal que $carac(F) = p$. Demostrar que existe un entero positivo n tal que $card(F) = p^n$.*

$\equiv$

La resolución de este ejercicio es una adaptación de un comentario que aparece en [6, p.218].

De un ejercicio anterior sabemos que existe un homomorfismo de cuerpos f entre $\mathbf{Z}_p$ y F que es inyectivo. Entonces $f(\mathbf{Z}_p)$ es un subcuerpo de F que es isomorfo a $\mathbf{Z}_p$. Sea $n := [F : f(\mathbf{Z}_p)]$. Así, existe una base $B = \{a_1, a_2, ..., a_n\}$ de F sobre $f(\mathbf{Z}_p)$. Definimos ahora la aplicación

$$\begin{array}{rccl} \varphi & : & F \longrightarrow & f(\mathbf{Z}_p) \times f(\mathbf{Z}_p) \times \overset{(n)}{\cdots} \times f(\mathbf{Z}_p) \\ & a & \to & \varphi(a) := (x_1, x_2, ..., x_n) \ / \ a = x_1a_1 + x_2a_2 + ... + x_na_n \end{array}$$

La aplicación φ está bien definida, ya que, para cada $a \in F$, sus coordenadas en la base B sabemos son únicas. Además, φ es obviamente inyectiva y sobre. Es decir, φ es una biyección, por lo que

$$card(F) = card(f(\mathbf{Z}_p) \times \overset{(n)}{\cdots} \times f(\mathbf{Z}_p)) = card(\mathbf{Z}_p \times \overset{(n)}{\cdots} \times \mathbf{Z}_p) = card(\mathbf{Z}_p)^n = p^n. \ \clubsuit$$

2.2. Polinomios sobre un cuerpo

Ex. 169 *Sea F un cuerpo. Representamos, como es habitual, por $F[x]$ al dominio de integridad de los polinomios de indeterminada x con coeficientes en F, es decir*

$$F[x] = \{ f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n : \ n \in \mathbf{N} \cup \{0\}, a_0, a_1, ..., a_n \in F\}.$$

Sea $F(x) := \{ \frac{f(x)}{g(x)} : \ f(x), g(x) \in F[x], g(x) \neq 0\}$. En $F(x)$ introducimos las operaciones

$$\begin{array}{ll} \underline{\text{Suma}} : & \frac{f(x)}{g(x)} + \frac{u(x)}{v(x)} = \frac{f(x)v(x)+g(x)u(x)}{g(x)v(x)} \\ \underline{\text{Producto}} : & \frac{f(x)}{g(x)} \cdot \frac{u(x)}{v(x)} = \frac{f(x)u(x)}{g(x)v(x)}. \end{array}$$

Demostrar que $F(x)$ es un cuerpo extensión de F [el cuerpo de las funciones racionales].

$\equiv$

Antes de ponernos a resolver, recordemos que un domino de integridad es una estructura bioperativa $(D, +, \cdot)$ que cumple:

1) $(D, +)$ es un grupo abeliano.
2) La segunda operación $\cdot$ (usualmente llamada "producto") ha de cumplir
   (2.1) Estable, o ley de composición interna.

(2.2) Asociativa.

(2.3) Distributiva respecto de $+$.

Cumpliendo sólo ésto, se dice que $(D, +, \cdot)$ tiene estructura de anillo.

(2.4) Neutro, al que se le suele llamar unidad (y se dice que tenemos un anillo unitario).

(2.5) No ha de tener divisores de cero y entonces se llama anillo íntegro. Dos elementos $a, b \in D$ son divisores de cero si cumplen: $a \neq 0$ (el neutro de $+$), $b \neq 0$, $a \cdot b = 0$. Observar que tener divisores de cero no es interesante, mas bien patológico.

(2.6) Conmutativa.

Es fácil comprobar que el conjunto de los polinomios sobre un cuerpo F, $F[x]$, dotado de las usuales operaciones de suma y producto polinómicos, es un dominio de integridad.

Procedemos a continuación a resolver el ejercicio. En realidad, un cuerpo no esmás que un dominio de integridad que además cumple que todo elemento no nulo admite inverso, o sea, simétrico para $\cdot$. De hecho, esta última propiedad implica ser íntegro. Por tanto

1) $(F(x), +)$ es un grupo abeliano. Se demuesta directamente, con un poco de paciencia (sumar fracciones).

2) La segunda operación $\cdot$ cumple (verficarlo, multiplicando fracciones)

(2.1) Estable.

(2.2) Asociativa.

(2.3) Distributiva.

(2.4) Unidad: $1 \in F(x)$.

(2.5) Inversos (para elementos no nulos).

(2.6) Conmutativa.

Finalmente, para ver que $F(x)$ es una extensión de F, basta con observar que $F \subset F(x)$, pues

$$a \in F \quad \rightarrow \quad a \in F[x] \quad \rightarrow \quad a = \frac{a}{1} \in F(x). \clubsuit$$

Ex. 170 *En* $\mathbf{Z}[x]$*, demostrar que, dados* $f, g \in \mathbf{Z}[x]$*,* g *mónico, existen únicos* $q, r \in \mathbf{Z}[x]$ *tales que*

$$f = q \cdot g + r, \quad grad(r) < grad(g). \quad \text{[División polinómica]}$$

$\equiv$

Como hacemos casi siempre, primero aclaremos ciertas cosas. Un polinomio $a_0 + a_1 x + ... + a_n x^x \in F[x]$, F cuerpo, $a_0, a_1, ..., a_n \in F$, $a_n \neq 0$, es mónico cuando $a_n = 1$, es decir, cuando su coeficiente director, o principal es la unidad. El grado de un polinomio es el mayor exponente de la indeterminada corrspondiente a un coeficiente distinto de cero si el polinomio no es el 0, por definición el grado del polinomio cero es $-\infty$. La demostración de lo pedido sigue un argumento standard. Consideramos el conjunto

$$H := \{ f - hg : h \in \mathbf{Z}[x] \}.$$

Si $0 \in H$, entonces existe $h \in \mathbf{Z}[x]$ tal que $0 = f - hg$, lo que implica que $f = hg$. Tomando $q := h$, $r := 0$, hemos terminado.

Supongamos pues que $0 \notin H$. Entonces $\{grad(u) : u \in H\} \subset \mathbf{N} \cup \{0\}$ y podemos garantizar la existencia de algún polinomio $r \in H$ tal que $grad(r)$ sea el mínimo de los grados de los polinomios de H. Como $r \in H$, existe $q \in \mathbf{Z}[x]$ de modo que $r = f - qg$. Claramente, $f = qg + r$, por lo que veamos que $grad(r) < grad(g)$. Por comodidad, llamemos $m := grad(r)$, $n := grad(g)$. Suponiendo que $m \geq n$, si $r = a_0 + a_1x + ... + a_mx^m$, consideremos el polinomio $u := r - a_mx^{m-n}g \in \mathbf{Z}[x]$. Entonces

$$u = r - a_mx^{m-n}g = f - qg - a_mx^{m-n}g = f - (q + a_mx^{m-n})g \in H.$$

Pero, como g es mónico, si $g = c_0 + c_1x + ... + c_{n-1}x^{n-1} + x^n$,

$$u = r - a_mx^{m-n}g = a_0 + a_1x + ... + a_mx^m - a_mx^{m-n}(c_0 + c_1x + ... + c_{n-1}x^{n-1}) - a_mx^{m-n}x^n$$

$$= a_0 + a_1x + ... + a_{m-1}x^{m-1} - a_mx^{m-n}(c_0 + c_1x + ... + c_{n-1}x^{n-1}),$$

lo que implica que $grad(u) \leq m - 1$, que es una contradicción.

Finalmente, veamos la unicidad de los polinomios q, r. Supongamos que existen $u, v \in \mathbf{Z}[x]$ ales que

$$\left.\begin{array}{rcll} f & = & q \cdot g + r, & grad(r) < grad(g) \\ f & = & u \cdot g + v, & grad(v) < grad(g) \end{array}\right\} \Rightarrow (q - u)g = r - v.$$

Entonces, si $q - u = 0$, hemos terminado, pues $q = u$, $r = v$. Si, en caso contrario, $q - u \neq 0$, tendríamos

$$grad(g) \leq grad(q - u) + grad(g) = grad(r - v) \leq \text{máx}\{grad(r), grad(v)\} < grad(g),$$

lo que es absurdo. ♣

Ex. 171 *Sea* $f(x) = c_0 + c_1x + c_2x^2 + ... + c_nx^n \in F[x]$ *un polinomio. Se define el polinomio derivada de* $f(x)$ *como* $f'(x) = c_1 + 2c_2x + 3c_3x^2 + ... + nc_nx^{n-1}$. *Demostrar que* $a \in F$ *es raíz de* $f(x)$ *y de* $f'(x)$ *si y sólo si* $(x - a)^2$ *divide a* $f(x)$.

≡

[$\Rightarrow$] Si a es raíz de $f(x)$, entonces, aplicando el algoritmo de la división en $F[x]$, existen $g(x) \in F[x]$, $r \in F$, tales que $f(x) = (x - a) \cdot g(x) + r$. Así

$$0 = f(a) = 0 \cdot g(a) + r = r \Rightarrow f(x) = (x - a)g(x) \Rightarrow f'(x) = g(x) + (x - a)g'(x).$$

De nuevo usando el algoritmo de la división polinómica en $F[x]$, existen $h(x) \in F[x]$, $s \in F$, tales que $g(x) = (x - a) \cdot h(x) + s$. Como a también es raíz de $f'(x)$

$$0 = f'(a) = g(a) + 0 \cdot g'(a) = g(a) = s \Rightarrow g(x) = (x - a)h(x) \Rightarrow f(x) = (x - a)^2h(x).$$

[$\Leftarrow$] Si $(x - a)^2$ es un divisor de $f(x)$, entonces existe $g(x) \in F[x]$ tal que $f(x) = (x - a)^2 \cdot g(x)$. Entonces, claramente $f(a) = 0$, y

$$f'(x) = 2(x - a)g(x) + (x - a)^2g'(x) \Rightarrow f'(a) = 0. \clubsuit$$

Ex. 172 *Dados los pares de elementos* $(a_0, b_0); (a_1, b_1); ...; (a_n, b_n)$ *de* $F \times F$, *con* $a_0, a_1, ..., a_n$ *distintos, demostrar que existe un único polinomio* $f(x) \in F[x]$ *de grado* n *que cumple que:* $f(a_i) = b_i$, $0 \leq i \leq n$. *[Teorema de interpolación de LaGrange]*

$\equiv$

Empleamos el método de los coeficientes indeterminados. Llamado $f(x) = c_0 + c_1 x + c_2 x^2 + ... + c_n x^n$ al polinomio buscado, con $c_i \in F$, $0 \leq i \leq n$, vamos a determinar dichos coeficiente. A partir de las $n+1$ condiciones $f(a_i) = b_i$, $0 \leq i \leq n$, obtenemos el sistema de $n+1$ ecuaciones con $n+1$ incógnitas siguiente

$$\begin{array}{rcl} c_0 + c_1 a_0 + c_2 a_0^2 + ... + c_n a_0^n & = & b_0 \\ c_0 + c_1 a_1 + c_2 a_1^2 + ... + c_n a_1^n & = & b_1 \\ ..... & & \\ ..... & & \\ c_0 + c_1 a_n + c_2 a_n^2 + ... + c_n a_n^n & = & b_n. \end{array}$$

Todo se reduce a ver que el sistema anterior es compatible determinado. Pero, como estos cálculos son análogos en el cuerpo F que en cualquier cuerpo numérico, ello equivale a ver que el siguiente determinante de Vandermonde de orden $n+1$ es distinto de cero

$$\begin{vmatrix} 1 & a_0 & a_0^2 & ... & a_0^n \\ 1 & a_1 & a_1^2 & ... & a_1^n \\ ..... & & & & \\ ..... & & & & \\ 1 & a_n & a_n^2 & ... & a_n^n \end{vmatrix} = \text{(puede verse inductivamente)} \prod_{0 \leq i < j \leq n} (a_i - a_j) \neq 0,$$

pues los elementos $a_0, a_1, ..., a_n$ son distintos y F es un cuerpo. ♣

Ex. 173 *Sea* F *un cuerpo con* q *elementos. Demostrar que todo elemento de* F *es raíz del polinomio* $x^q - x$.

$\equiv$

Podemos escribir F como $F = \{0, a_1, a_2, ..., a_{q-1}\}$. Claramente, 0 es raíz del polinomio. Para $i = 1, 2, ..., q-1$, como $a_i \in F^*$ y F^* es un grupo multiplicativo, está claro que

$$o(a_i) \mid o(F^*) = q - 1 \Rightarrow a_i^{q-1} = 1 \Rightarrow a_i^q - a_i = a_i(a_i^{q-1} - 1) = 0. \clubsuit$$

Ex. 174 *Sea* F *un cuerpo finito. Contando el número de elementos de* F^* *que son raíces del polinomio* $x^n - 1$ *para ciertos valores de* n, *demostrar que el grupo multiplicativo* F^* *es cíclico.*

$\equiv$

Sea $o(F^*) = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$ la factorización del orden de F^* en números primos. De ejercicios de teoría de grupos sabemos que $F^* = H_1 H_2 ... H_k$, con $o(H_i) = p_i^{m_i}$, $1 \leq i \leq k$. También de un ejercicio relativo a grupos, sabemos que todo se reduce a ver que cada subgrupo H_i, $1 \leq i \leq k$, es cíclico. Veamos que H_1 es cíclico, los demás se demuestran de

manera análoga. Para ello, ya que estamos trabajando con grupos abelianos, en virtud de otro ejercicio resuelto anteriormente correspondiente a la teoría de grupos, basta con ver que, si G_1 y G_2 son dos subgrupos de H_1, entonces o bien $G_1 \subset G_2$, o bien $G_2 \subset G_1$.

Como los órdenes de G_1 y de G_2 dividen al orden de H_1, que es $p_1^{m_1}$, supongamos que $o(G_1) = p_1^{n_1}$ y $o(G_2) = p_1^{n_2}$, con $n_1 \leq n_2$. Para ver que $G_1 \subset G_2$, lo que hacemos es demostrar que $G_1 = \{a \in F^* : \ a^{p_1^{n_1}} - 1 = 0\}$ y que $G_2 = \{a \in F^* : \ a^{p_1^{n_2}} - 1 = 0\}$, entonces la inclusión deseada es evidente. De nuevo, por comodidad, sólo probamos la primera igualdad (la otra es similar). También para más comodidad llamamos $d := p_1^{n_1}$. Sea $A := \{a \in F^* : \ a^d - 1 = 0\}$. Como A es el conjunto de todas las raíces en F del polinomio $x^d - 1$, está claro que $card(A) \leq d$. Sea D el conjunto de los enteros positivos divisores de d. Para $q \in D$, sea $B_q := \{a \in F^* : \ o(a) = q\}$. Veamos que $A = \cup_{q \in D} B_q$:
$[\subset]$ Si $a \in A$, entonces $1 = a^d$, de donde $o(a) \mid d$, i.e., $o(a) \in D$, llamado $q := o(a)$, se tiene que $a \in B_q$.
$[\supset]$ Si $a \in B_q$, para algún $q \in D$, se tiene que $a^d - 1 = (a^q)^{\frac{d}{q}} - 1 = 1 - 1 = 0$, por lo que $a \in A$.

Consideramos ahora $i \in \mathbf{N}$ tal que i es menor que q y primo con q. Entonces

$$o(a^i) \ = \ \frac{q}{mcd(i,q)} \ = \ q \ \Rightarrow \ a^i \in \ B_q.$$

Por tanto, $card(B_q) \geq \Phi(d)$, siendo Φ la función de Euler, de la que hemos hablado en ejercicios anteriores. Así, como los conjuntos B_q, $q \in D$, son disjuntos dos-a-dos,

$$d \ \geq \ card(A) \ = \ card(\cup_{q \in D} B_q) \ = \ \sum_{q \in D} card(B_q) \ \geq \ \sum_{q \in D} \Phi(q) \ = \ d,$$

i.e., $card(A) = d$. Consecuentemente, como $G_1 \subset A$ y $card(A) = d = o(G_1)$, se deduce que $G_1 = A$, como queríamos. ♣

Ex. 175 *Si p es primo, construir un isomorfismo de grupos entre el grupo aditivo $\mathbf{Z}_{p-1}$ y el grupo multiplicativo $\mathbf{Z}'_p$.*

≡

Recordemos que

$$\mathbf{Z}_{p-1} \ = \ \{ \overline{0}, \overline{1}, ..., \overline{p-2} \}; \quad \mathbf{Z}'_p \ = \ \{ \overline{k} \in \mathbf{Z}_p : \ mcd(k,p) = 1\} \ = \ \{ \overline{1}, \overline{2}, ..., \overline{p-1} \}.$$

Al ser $\mathbf{Z}_p$ un cuerpo (puesto que p es primo), sabemos que $\mathbf{Z}_p^* = \mathbf{Z}'_p$ es un grupo multiplicativo cíclico, por tanto, existe $\overline{i} \in \mathbf{Z}'_p$ tal que $\mathbf{Z}'_p = \langle \overline{i} \rangle$, con $o(\overline{i} = o\mathbf{Z}'_= p - 1$. Así definimos

$$\begin{array}{rccc} f & : & \mathbf{Z}_{p-1} & \longrightarrow & \mathbf{Z}'_p \\ & & \overline{k} & \to & f(\overline{k}) = \overline{i}^{\,k}. \end{array}$$

f bien definida: Sean $\overline{k}, \overline{j} \in \mathbf{Z}_{p-1}$ tales que $\overline{k} = \overline{j}$. Entonces, existe un entero n de modo que $k - j = n(p-1)$. Por tanto

$$f(\overline{k}) = \overline{i}^{\,k} \ = \ \overline{i}^{\,j+n(p-1)} \ = \ \overline{i}^{\,j} \cdot \overline{i}^{\,n(p-1)} \ = \ \overline{i}^{\,j} \cdot (\overline{i}^{p-1})^n \ = \ \overline{i}^{\,j} \cdot \overline{1} \ = \ \overline{i}^{\,j} \ = \ f(\overline{j}).$$

f homomorfismo de grupos: Sean $\overline{k}, \overline{j} \in \mathbf{Z}_{p-1}$.

$$f(\overline{k}+\overline{j}) \;=\; f(\overline{k+j}) \;=\; \overline{i}^{\,k+j} \;=\; \overline{i}^{\,k} \cdot \overline{i}^{\,j} \;=\; f(\overline{k}) \cdot f(\overline{j}).$$

f inyectiva: Sea $\overline{k} \in Ker(f)$, podemos tomar $0 \leq k < p-1$. Entonces

$$\overline{1} \;=\; f(\overline{k}) \;=\; \overline{i}^{\,k} \;\Rightarrow\; p-1 \mid k \;\Rightarrow\; k=0 \;\Rightarrow\; \overline{k}=\overline{0}.$$

Como $\mathbf{Z}_{p-1}$ y $\mathbf{Z}'_p$ son finitos del mismo cardinal, se tiene que f es una biyección. ♣

Ex. 176 *Para p primo, demostrar que* $(p-1)! \equiv -1 \;\; (mod.\ p)$.
[Teorema de Sir John Wilson (1741-1793)]

≡

Este es un problema bonito y muy útil en Teoría de Números. Como hicimos antes, al ser p primo tenemos que $\mathbf{Z}_p$ es un cuerpo y por tanto $\mathbf{Z}'_p = \mathbf{Z}^*_p = \{\overline{1}, \overline{2}, ..., \overline{p-1}\}$ es un grupo multiplicativo cíclico. Consideremos el polinomio

$$f(x) \;=\; x^{p-1} - \overline{1} \;\in\; \mathbf{Z}_p[x]\ .$$

Claramente, todo elemento de $\overline{k} \in \mathbf{Z}'_p$ cumple que $\overline{k}^{\,p-1} = \overline{1}$, por lo que los $p-1$ elementos de $\mathbf{Z}'_p$ son raíces de $f(x)$ y, como este polinomio es de grado $p-1$, queda claro que se trata de la únicas raíces de $f(x)$. Así, como es un polinomio mónico, factoriza del siguiente modo

$$f(x) \;=\; (x-\overline{1})(x-\overline{2})...(x-(\overline{p-1})).$$

Ello implica que, observando que $p-1$ es par,

$$\left.\begin{array}{l} f(\overline{0}) \;=\; -\overline{1} \\ f(\overline{0}) = (-\overline{1})(-\overline{2})...(-(\overline{p-1})) = (-1)^{p-1}\overline{(p-1)!} = \overline{(p-1)!} \end{array}\right\}$$

$$\Rightarrow \;\; -\overline{1} \;=\; \overline{(p-1)!} \;\Rightarrow\; (p-1)! \;\equiv\; -1 \;(mod.\ p). \;\clubsuit$$

Ex. 177 *Demostrar que si un polinomio* $f(x) = c_0 + c_1 x + ... + c_n x^n \in \mathbf{Z}[x]$ *tiene una raíz en* $\frac{p}{q} \in \mathbf{Q}$, *con* $mcd(p,q) = 1$ *(i.e.* $\frac{p}{q}$ *es una fracción irreducible), entonces* $p \mid c_0$ *y* $q \mid c_n$. *[Interesante para una aplicación inteligente de la Regla de Ruffini (Paolo)]*

≡

De

$$0 \;=\; f(\frac{p}{q}) \;=\; c_0 + c_1 \cdot \frac{p}{q} + c_2 \cdot (\frac{p}{q})^2 + ... + c_n \cdot (\frac{p}{q})^n,$$

multiplicando ambos miembros por q^n

$$\begin{aligned} 0 \;&=\; c_0 q^n + c_1 p q^{n-1} + c_2 p^2 q^{n-2} + ... + c_n p^n \;\Rightarrow\; -c_0 q^n \\ &=\; (c_1 q^{n-1} + c_2 p q^{n-2} + ... + c_{n-1} p^{n-2} q + c_n p^{n-1})\ p \\ &\Rightarrow\; p \mid -c_0 q^n \overset{(mcd(p,q)=1)}{\Rightarrow} p \mid c_0. \end{aligned}$$

Análogamente, despejando de otra forma

$$-c_n p^n \;=\; q\ (c_0 q^{n-1} + c_1 p q^{n-2} + ... + c_{n-1} p^{n-1}) \;\Rightarrow\; q \mid -c_n p^n \;\Rightarrow\; q \mid c_n. \;\clubsuit$$

Ex. 178 *Sea F un cuerpo y $f(x)$ un polinomio de $F[x]$ cuyo polinomio derivada cumple que $f'(x) = 0$.*

a) Demostrar que, si $carac(F) = 0$, entonces existe un $a \in F$ tal que $f(x) = a$, i.e., $f(x)$ es un polinomio constante.

b) Qué se puede decir si $carac(F) \neq 0$?

≡

a) Sean

$$\begin{aligned} f(x) &= c_0 + c_1 x + c_2 x^2 + ... + c_n x^n \\ f'(x) &= c_1 + 2c_2 x + 3c_3 x^2 + ... + nc_n x^{n-1}. \end{aligned}$$

Como $f'(x) = 0$, todos los coeficientes de $f'(x)$ son nulos, es decir

$$\left.\begin{array}{l} 0 = c_1 \\ 0 = 2c_2 \overset{(carac(F)=0)}{\rightarrow} c_2 = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0 = nc_n \overset{(carac(F)=0)}{\rightarrow} c_n = 0 \end{array}\right\} \Rightarrow f(x) = c_0 \in F.$$

b) Si $carac(F) = p \neq 0$, veamos que siempre hay un polinomio de grado p cuya derivada es nula: Basta tomar $f(x) = x^p$. Entonces

$f(x)$ no es constante

$f'(x) = p\, x^{p-1} \overset{(carac(F)=p)}{\rightarrow} \forall a \in F,\ f'(a) = p \cdot 1 = 0 \rightarrow f'(x) = 0.$ ♣

Ex. 179 *Demostrar que todo polinomio de $\mathbf{R}[x]$ puede factorizarse como un producto de polinomios de $\mathbf{R}[x]$ de grado 1 ó 2.*

≡

Empezamos demostrando un clásico resultado de la teoría de polinomios que nos va a servir para resolver el ejercicio, aunque por sí sólo este resultado es de gran importancia.

Lema 5 *Sea $f(x) \in \mathbf{R}[x]$. Si $z \in \mathbf{C}$ es raíz de $f(x)$ entonces el complejo conjugado $\overline{z}$ también es raíz de $f(x)$. Es decir, si un número complejo es raíz de un polinomio de coeficientes reales, también lo es el complejo conjugado.*

≡

Sea $f(x) = c_0 + c_1 x + ... + c_n x^n$, con $c_0, c_1, ..., c_n \in \mathbf{R}$. Entonces

$$0 = f(z) = c_0 + c_1 z + ... + c_n z^n \overset{(tomando\ conjugados)}{\Rightarrow} 0 = \overline{c_0 + c_1 z + ... + c_n z^n}$$

$$= \overline{c_0} + \overline{c_1 z} + ... + \overline{c_n z^n} = c_0 + c_1 \overline{z} + ... + c_n \overline{z}^n = f(\overline{z}).\ \bullet$$

Volviendo al ejercicio, recordemos que el Teorema Fundamental del Algebra dice que todo polinomio de $\mathbf{C}[x]$ se descompone totalmente en $\mathbf{C}$, i.e., admite tantos factores de primer grado (posiblemente repetidos) como indica su grado. Entonces, si $f(x) =$

$c_0 + c_1x + ... + c_nx^n \in \mathbf{R}[x] \subset \mathbf{C}[x]$, sean $z_1, z_2, ..., z_k \in \mathbf{C} \setminus \mathbf{R}$ (posiblemente repetidos), con $z_j = b_j + c_j i$, $1 \leq j \leq k$, y $a_1, a_2, ..., a_{n-2k} \in \mathbf{R}$ (posiblemente repetidos) tales que, en virtud del lema previo,

$$\begin{aligned} f(x) &= c_n(x-a_1)(x-a_2)...(x-a_{n-2k})(x-z_1)(x-\overline{z_1})...(x-z_k)(x-\overline{z_k}) \\ &= c_n(x-a_1)(x-a_2)...(x-a_{n-2k})[(x-b_1)^2+c_1^2]...[(x-b_k)^2+c_k^2]. \clubsuit \end{aligned}$$

Ex. 180 *Dados $f(x) \in \mathbf{C}[x]$ y $\omega \in \mathbf{C}$, se dice que ω es una raíz de $f(x)$ de multiplicidad m siempre que $(x-\omega)^m \mid f(x)$ y $(x-\omega)^{m+1} \not| f(x)$. Demostrar que ω es una raíz de $f(x)$ de multiplicidad m si y sólo si*

$$f(\omega) = f'(\omega) = ... = f^{(m-1)}(\omega) = 0, \quad f^{(m)}(\omega) \neq 0.$$

$\equiv$

$[\Rightarrow]$ Si ω es un complejo que es raíz del polinomio $f(x) \in \mathbf{C}[x]$ de multiplicidad m, por definición, existe $g(x) \in \mathbf{C}[x]$ tal que

$$f(x) = (x-\omega)^m \cdot g(x), \quad g(\omega) \neq 0.$$

Para $n = 1, 2, ..., m-1$, usando la fórmula de Leibnitz

$$f^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} [(x-\omega)^m]^{(k)} g^{(n-k)}(x) = \sum_{k=0}^{n} \binom{n}{k} \frac{m!}{(m-k)!}(x-\omega)^{m-k} g^{(n-k)}(x)$$

$$= (x-\omega)\sum_{k=0}^{n} \binom{n}{k} \frac{m!}{(m-k)!}(x-\omega)^{m-k-1} g^{(n-k)}(x).$$

Así, para $n = 0, 1, ..., m-1$, es evidente que $f^{(n)}(\omega) = 0$. Además

$$f^{(m)}(x) = \sum_{k=0}^{m} \frac{m!}{k!(m-k)!}\frac{m!}{(m-k)!}(x-\omega)^{m-k} g^{(m-k)}(x)$$

$$= \sum_{k=0}^{m-1} \frac{m!}{k!(m-k)!}\frac{m!}{(m-k)!}(x-\omega)^{m-k} g^{(m-k)}(x) + m!g(x),$$

de donde $f^{(m)}(\omega) = m!g(\omega) \neq 0$.

$[\Leftarrow]$ Partiendo de que

$$f(\omega) = f'(\omega) = ... = f^{(m-1)}(\omega) = 0, \quad f^{(m)}(\omega) \neq 0,$$

deducimos

$$f(\omega) = 0 \overset{(Teorema\ del\ resto)}{\rightarrow} \exists g_1(x) \in \mathbf{C}[x] \ / \ f(x) = (x-\omega) \cdot g_1(x).$$

Como $f'(x) = g_1(x) + (x-\omega)g_1'(x)$,

$f'(\omega) = 0 \rightarrow g_1(\omega) = 0 \rightarrow \exists g_2(x) \in \mathbf{C}[x] \ / \ g_1(x) = (x-\omega)\cdot g_2(x) \rightarrow f(x) = (x-\omega)^2 g_2(x)$.

Repitiendo este proceso obtenemos que

$$\exists g_m(x) \in \mathbf{C}[x]/\ f(x) = (x-\omega)^m \cdot g_m(x).$$

Por tanto, hemos demostrado que $(x-\omega)^m \mid f(x)$. Finalmente, suponiendo que $(x-\omega)^{m+1}$ fuese divisor de $f(x)$, como $f(x) = (x-\omega)^m \cdot g_m(x)$, se tendría que $(x-\omega) \mid g_m(x)$. Pero ello implica que $g_m(\omega) = 0$ y entonces

$$f^{(m)}(x) = \sum_{k=0}^{m} \frac{m!}{k!(m-k)!}\frac{m!}{(m-k)!}(x-\omega)^{m-k} g_m^{(m-k)}(x)$$

$$= \sum_{k=0}^{m-1} \frac{m!}{k!(m-k)!}\frac{m!}{(m-k)!}(x-\omega)^{m-k} g_m^{(m-k)}(x) \ + \ m! g_m(x),$$

así $f^{(m)}(\omega) = m! g_m(\omega) = 0$, lo que contradice una de nuestras hipótesis de partida. ♣

Ex. 181 *Demostrar que todo polinomio irreducible de* $\mathbf{R}[x]$ *es de grado* 1 *ó* 2.

≡

Recordemos que, si F es un cuerpo, un polinomio $f(x) \in F[x]$, de grado mayor o igual que 1, es irreducible, o primo, siempre que los únicos divisores que admite en $F[x]$ son o bien constantes, i.e., elementos de F, o bien polinomios asociados a $f(x)$, i.e., de la forma $g(x) = a \cdot f(x)$, $a \in F$. Supongamos que $f(x) \in \mathbf{R}[x]$ es irreducible y tiene grado mayor o igual que 3. Haciendo uso de un ejercicio resuelto anteriormente, sabemos que $f(x)$ factoriza en polinomios de grado 1 o de grado 2. Ello significa que admite factores que ni son constantes ni tienen el grado de $f(x)$, es decir, $f(x)$ sería reducible. ♣

Ex. 182 *Demostrar que todo polinomio de grado positivo sobre un cuerpo* F *es divisible por un polinomio irreducible sobre* F.

≡

Sea $f(x) \in F[x]$ y sea $n \geq 1$ el grado de $f(x)$. Hacemos la demostración por recurrencia (inducción) sobre el grado n. Para $n = 1$, la afirmación es obviamente cierta ya que todo polinomio de grado 1 es irreducible. Suponiendo que la afirmación vale para todo polinomio de grado menor que n, veamos su validez cuando el grado del polinomio $f(x)$ es n. Podemos suponer tranquilamente que $f(x)$ es reducible (de ser irreducible, como $f(x) \mid f(x)$, habríamos terminado). Entonces existen $g(x), h(x) \in F[x]$ tales que

$$f(x) = g(x) \cdot h(x), \quad 1 \leq grado(g) < n, \quad 1 \leq grado(h) < n\ .$$

Aplicando la hipótesis de recurrencia al polinomio $g(x)$ (o a $h(x)$), tenemos que $g(x)$ admite un divisor irreducible sobre F. Consecuentemente, ese mismo divisor irreducible sobre F divide también a $f(x)$. ♣

Ex. 183 *Demostrar que existe un número infinito de polinomios irreducibles sobre cualquier cuerpo.*

≡

Dado un cuerpo F, para demostrar que $F[x]$ contiene infinitos polinomios irreducibles vamos a usar el mismo argumento que ya utilizó Euclides (varios siglos antes de Cristo) para demostrar la existencia de infinitos números primos. Razonando por reducción al absurdo, supongamos que hay una cantidad finita en $F[x]$ de polinomios irreducibles. Vamos a representarlos por

$$f_1(x),\ f_2(x),\ ...,\ f_n(x)\ .$$

Consideramos ahora el polinomio

$$g(x)\ :=\ f_1(x)\cdot f_2(x)\cdot ...\cdot f_n(x)\ +\ 1\ .$$

Claramente $g(x) \in F[x]$ y, como todos los polinomios irreducibles son los de arriba, sabemos que alguno de ellos debe ser un divisor de $g(x)$. Supongamos (comodidad) que $f_1(x) \mid g(x)$. Entonces existe $h(x) \in F[x]$ tal que

$$g(x)\ =\ f_1(x)\cdot h(x)\ \Rightarrow\ 1\ =\ f_1(x)[h(x)\ -\ f_2(x)...f_n(x)],$$

lo que no puede ser, ya que el grado de $f_1(x)$ (y de cualquier polinomio irreducible) es positivo y el grado de un producto es la suma de los grados. ♣

Ex. 184 *Calcular el número de polinomios irreducibles de grados* 1, 2 *y* 3 *de* $\mathbf{Z}_p[x]$.

≡

Aunque no va a influir en la resolución del ejercicio, recordar que p ha de ser primo, par que Z_p sea un cuerpo. Lo hacemos por grados. Para mayor claridad, consideramos el conjunto siguiente, dado $n \in \mathbf{N}$,

$$\mathcal{I}_n\ :=\ \{\ f(x) \in \mathbf{Z}_p[x]\quad f(x) \text{ tiene grado n y es irreducible }\}.$$

Grado 1: En este caso

$$\mathcal{I}_1\ :=\ \{\ ax+b \in \mathbf{Z}_p[x]\quad a,b \in F,\ a \neq 0\ \}\ \Rightarrow\ card(\mathcal{I}_1)\ =\ (p-1)p.$$

Grado 2: Ahora, si llamamos $\mathbf{Z}_p[x]_2$ al conjunto de los polinomios de $\mathbf{Z}_p[x]$ que tienen grado 2 y $\mathcal{R}_2$ al subconjunto de $\mathbf{Z}_p[x]_2$ formado por los que son reducibles, claramente tenemos que

$$\mathbf{Z}_p[x]_2\ =\ \mathcal{I}_2\ \cup\ \mathcal{R}_2,\qquad \mathcal{I}_2\ \cap\ \mathcal{R}_2\ =\ \emptyset.$$

Así, si $f(x) \in \mathcal{R}_2$, entonces $f(x) = a(x-b)(x-c)$, $a,b,c \in F$, $a \neq 0$. Por tanto

$$card(\mathcal{R}_2)\ =\ (p-1)\cdot CR_{p,2}\ =\ (p-1)\cdot \left(\begin{array}{c} p+1 \\ 2 \end{array}\right).$$

Nota 19 La notación $CR_{p,2}$ significa combinaciones con repetición de p objetos tomados de 2 en 2. En general, la fórmula de cálculo del número de combinaciones con repetición de p objetos tomados de k en k es

$$CR_{p,k}\ =\ \left(\begin{array}{c} p+k-1 \\ k \end{array}\right).$$

Por tanto

$$card(\mathcal{I}_2) = card(\mathbf{Z}_p[x]_2) - card(\mathcal{R}_2) = (p-1)p^2 - (p-1)\cdot\begin{pmatrix} p+1 \\ 2 \end{pmatrix}$$

$$= (p-1)\,[p^2 - \frac{(p+1)p}{2}] = \frac{1}{2}\,p\,(p-1)^2.$$

Grado 3: Utilizando una notación similar a la anterior, es evidente que $card(\mathbf{Z}_p[x]_3) = (p-1)p^3$. Además, si $f(x) \in \mathcal{R}_3$, entonces, como ha de tener alguna raíz en F, se tiene que

$$f(x) = \begin{cases} a(x-b)(x-c)(x-d), & a,b,c,d \in F,\ a \neq 0 \\ a(x-b)(x^2+cx+d), & a,b \in F,\ a \neq 0,\ x^2+cx+d \in \mathcal{I}_2. \end{cases}$$

Así

$$card(\mathcal{R}_3) = (p-1)\cdot CR_{p,3} + (p-1)\frac{card(\mathcal{I}_2)}{p-1} = (p-1)\cdot\begin{pmatrix} p+2 \\ 3 \end{pmatrix} + (p-1)p\frac{1}{2}p(p-1)$$

$$= (p-1)\,[\frac{(p+2)(p+1)p}{6} + \frac{p^2(p-1)}{2}] = \frac{1}{3}\,p(p-1)(2p^2+1).$$

Finalmente

$$card(\mathcal{I}_3) = (p-1)p^3 - \frac{1}{3}\,p(p-1)(2p^2+1) = \frac{1}{3}\,p(p-1)^2(p+1). \clubsuit$$

Ex. 185 *Determinar todos los polinomios mónicos de* $\mathbf{Z}_3[x]$ *de grados* 2 *y* 3 *que son irreducibles.*

≡

Como antes, vamos por grados. Por comodidad, escribimos el cuerpo $\mathbf{Z}_3 = \{0,1,2\}$, donde se entiende que la suma y producto se hacen módulo 3. También en aras de mayor comodidad, si un polinomio $f(x) = x^2 + ax + b \in \mathbf{Z}_3[x]_2$, lo representamos por $(1, a, b)$, análogamente para los de $\mathbf{Z}_3[x]_3$.

Grado 2: Lo hacemos claro, vamos a escribir todos los elementos mónicos de $\mathbf{Z}_3[x]_2$ indicando cuáles son irreducibles (irred) y cuáles son reducibles (red).

$$\overset{(red)}{(1,0,0)};\ \overset{\textbf{(irred)}}{\mathbf{(1,0,1)}};\ \overset{(red)}{(1,0,2)};\ \overset{(red)}{(1,1,0)};\ \overset{(red)}{(1,1,1)};\ \overset{\textbf{(irred)}}{\mathbf{(1,1,2)}};\ \overset{(red)}{(1,2,0)};\ \overset{(red)}{(1,2,1)};\ \overset{\textbf{(irred)}}{\mathbf{(1,2,2)}}.$$

Llamando correlativamente $f_1(x), f_2(x), ..., f_9(x)$ a los 9 elementos escritos arriba, vamos uno por uno a verificar lo afirmado.

$f_1(x) = x^2$ es reducible: $f_1(x) = x^2 = x \cdot x$.

$f_2(x) = x^2 + 1$ es **irreducible**: De ser reducible admitiría alguna raíz en $\mathbf{Z}_3$, pero $f_2(0) = 1$, $f_2(1) = 2$, $f_2(2) = 2$.

$f_3(x) = x^2 + 2$ es reducible: $f_3(1) = 0$ implica que $x - 1$ divide a $f_3(x)$. De hecho, $x^2 + 2 = (x-1)(x-2)$.

$f_4(x) = x^2 + x$ es reducible: $x^2 + x = x(x+1)$.

$f_5(x) = x^2 + x + 1$ es reducible: $f_5(1) = 0$.
$f_6(x) = x^2 + x + 2$ es **irreducible**: $f_6(0) = 2$, $f_6(1) = 1$, $f_6(2) = 2$.
$f_7(x) = x^2 + 2x$ es reducible: $x^2 + 2x = x(x + 2)$.
$f_8(x) = x^2 + 2x + 1$ es reducible: $f_8(2) = 0$.
$f_9(x) = x^2 + 2x + 2$ es **irreducible**: $f_9(0) = 2$, $f_9(1) = 2$, $f_9(2) = 1$.
Grado 3: Ahora la cosa es más variada. Si $f(x) = x^3 + ax^2 + bx + c \in \mathbf{Z}_3[x]_3$ queremos que sea irreducible, está claro que $c \neq 0$, i.e., $c \in \{1, 2\}$. Así distinguimos dos casos.
1) $c = 1$. Entonces $f(x) = x^3 + ax^2 + bx + 1$ y

$$f(x) \text{ irred } \Rightarrow \left\{ \begin{array}{l} a + b \neq 1 \text{ (si a + b = 1 } \rightarrow \text{ f(1) = 0} \\ a + 2b \neq 0 \text{ (si a + 2b = 0 } \rightarrow \text{ f(2) = 0} \end{array} \right\}$$

$\Rightarrow f(x) \in \{\mathbf{x^3 + 2x + 1},\ \mathbf{x^3 + x^2 + 2x + 1},\ \mathbf{x^3 + 2x^2 + 1},\ \mathbf{x^3 + 2x^2 + x + 1}\}$ todos irred.

2) $c = 2$. Entonces $f(x) = x^3 + ax^2 + bx + 2$ y

$$f(x) \text{ irred } \Rightarrow \left\{ \begin{array}{l} a + b \neq 0 \text{ (si a + b = 0 } \rightarrow \text{ f(1) = 0} \\ a + 2b \neq 2 \text{ (si a + 2b = 2 } \rightarrow \text{ f(2) = 0} \end{array} \right\}$$

$\Rightarrow f(x) \in \{\mathbf{x^3 + 2x + 2},\ \mathbf{x^3 + x^2 + 2},\ \mathbf{x^3 + x^2 + x + 2},\ \mathbf{x^3 + 2x^2 + 2x + 2}\}$ todos irred. ♣

Nota 20 Observar que lo obtenido en el ejercicio anterior es coherente con el resultado del ejercicio 184, ya que, como $p = 3$

$$card(\mathcal{I}_2) = \frac{1}{2}p(p-1)^2 = 6 : \{x^2+1, x^2+x+2, x^2+2x+2, 2(x^2+1), 2(x^2+x+2), 2(x^2+2x+2)\}$$

$$card(\mathcal{I}_3) = \tfrac{1}{3}p(p-1)^2(p\text{'}1) = 16 :$$
$$\{x^3 + 2x + 1,\ x^3 + x^2 + 2x + 1,\ x^3 + 2x^2 + 1,\ x^3 + 2x^2 + x + 1,$$
$$x^3 + 2x + 2,\ x^3 + x^2 + 2,\ x^3 + x^2 + x + 2,\ x^3 + 2x^2 + 2x + 2,$$
$$2(x^3 + 2x + 1), 2(x^3 + x^2 + 2x + 1), 2(x^3 + 2x^2 + 1), 2(x^3 + 2x^2 + x + 1),$$
$$2(x^3 + 2x + 2), 2(x^3 + x^2 + 2), 2(x^3 + x^2 + x + 2), 2(x^3 + 2x^2 + 2x + 2)\}.$$

Ex. 186 *Demostrar que $f(x)$ es irreducible en $F[x]$ si y sólo si, para cualquier $a \in F$, $f(x + a)$ es irreducible.*

≡
[⇐] Evidente, basta tomar $a = 0$.
[⇒] Si $a \in F$, llamamos $g(x) := f(x + a)$. De ser $g(x)$ reducible, existirían $p(x), q(x) \in F[x]$ tales que $g(x) = p(x)q(x)$, con $grado(p(x)) \geq 1$ y $grado(q(x)) \geq 1$. Entonces $f(x) = g(x - a) = p(x - a)q(x - a)$, de donde, como los polinomios $p(x - a), q(x - a)$ tienen los mismos grados que $p(x)$ y $q(x)$, se tendría que $f(x)$ es irreducible, lo que contradice la hipótesis de partida. ♣

Ex. 187 *Comprobar que $4x^3 - 3x - \frac{1}{2}$ es irreducible en $\mathbf{Q}[x]$.*

$\equiv$

Llamando $f(x) := 4x^3 - 3x - \frac{1}{2}$ y suponiendo que fuese reducible sobre $\mathbf{Q}$, está claro que admitiría alguna raíz $\frac{p}{q} \in \mathbf{Q}$, $p, q \in \mathbf{Z}$, $mcd(p,q) = 1$. Entonces

$$0 = f(\frac{p}{q}) = 4(\frac{p}{q})^3 - 3\frac{p}{q} - \frac{1}{2} \Rightarrow 8p^3 - 6pq^2 - q^3 = 0.$$

Ello implica que

$$p(8p^2 - 6q^2) = q^3 \Rightarrow p \mid q^3 \Rightarrow p \mid q \overset{(mcd(p,q)=1)}{\Rightarrow} p \in \{\pm 1\}.$$

Análogamente

$$q^2(6p+q) = 8p^3 \Rightarrow q^2 \mid 8p^3 \overset{(mcd(p,q)=1)}{\Rightarrow} q^2 \mid 8 \Rightarrow q^2 \in \{1,4\} \Rightarrow q \in \{\pm 1, \pm 2\}.$$

Consecuentemente $(p,q) \in \{\pm 1\} \times \{\pm 1, \pm 2\}$. Puede verse fácilmente que ninguna de las 8 fracciones posibles para $\frac{p}{q}$ obtenidas es raíz de $f(x)$, lo que supone un absurdo. ♣

Nota 21 Veamos otra forma de resolver el ejercicio anterior, esta vez haciendo uso del Criterio de Eisenstein. Este criterio de irreducibilidad sobre $\mathbf{Q}$ es conocido también como Teorema de Schönemann-Eisenstein y dice lo siguiente:

Sea $f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbf{Z}[x]$. Si existe un número primo p que cumple las siguientes tres condiciones:

1) $p \mid a_i, \quad 0 \leq i \leq n-1$
2) $p \not\mid a_n$
3) $p^2 \not\mid a_0$,

entonces $f(x)$ es irreducible sobre $\mathbf{Q}$.

Entonces, haciendo el cambio $x = \frac{y+1}{2}$, tenemos que

$$f(\frac{y+1}{2}) = 4\frac{y^3+3y^3+3y+1}{8} - 3\frac{y+1}{2} - \frac{1}{2} = \frac{1}{2}(y^3+3y^2-3).$$

Por tanto, $f(x)$ es irreducible si y sólo si lo es el polinomio $g(y) := y^3+3y^2-3$. Aplicando a $g(y)$ el criterio de Eisenstein, tomando $p := 3$, queda claro que se cumplen las tres condiciones

$$\left.\begin{array}{l} a_0 = -3,\ a_1 = 0,\ a_2 = 3,\ a_3 = 1 \\ 3 \mid a_0,\ \ 3 \mid a_1,\ \ 3 \mid a_2 \\ 3 \not\mid a_3 \\ 3^2 \not\mid a_0 \end{array}\right\} \Rightarrow g(y) = y^3+3y^2-3 \text{ es irreducible sobre } \mathbf{Q}.$$

También conviene resaltar que el polinomio $f(x) = 4x^3 - 3x - \frac{1}{2}$ es de cierta importancia, pues se emplea en la demostración de que es imposible construir el ángulo 20° con regla y compás. Es decir, se utiliza en la demostración de que 60° no se puede trisectar (dividir en tres ángulos iguales). Recordar que los problemas de la trisección del ángulo y el de la cuadratura del círculo (construir con regla y compás un cuadrado con la misma área que un círculo) son dos de los problemas clásicos que el hombre ha intentado resolver desde antaño.

Ex. 188 *Un número entero $m \in \mathbf{Z}$ se dice que es un residuo cuadrático módulo p, p primo, siempre que el polinomio $x^2 - \overline{m} \in \mathbf{Z}_p[x]$ tiene alguna raíz en $\mathbf{Z}_p$. Enumerar los elementos $\overline{m} \in \mathbf{Z}_p$ para los que $x^2 - \overline{m} \in \mathbf{Z}_p[x]$ tiene alguna raíz en $\mathbf{Z}_p$.*

$\equiv$

El ejercicio nos pide los valores $\overline{m} \in \mathbf{Z}_p$ tales que m es un residuo cuadrático módulo p. Vamos a demostrar que estos valores son exactamente

$$\begin{cases} \{\overline{0}, \overline{1}\}, & si \;\; p = 2, \\ \{\overline{0}, \overline{1}, \overline{4}, ..., (\overline{\frac{p-1}{2}})^2\}, & si \;\; p \neq 2. \end{cases}$$

Claramente, si estamos en $\mathbf{Z}_2[x]$, los polinomios $x^2 - \overline{0} = x^2$ y $x^2 - \overline{1} = (x - \overline{1})(x + \overline{1})$ admiten raíces y por ello $\{0, 1\}$ son residuos cuadráticos módulo 2. Si p es un primo distinto de 2, entonces la demostración requiere más cuidado.
$[\subset]$ Si $m \in \mathbf{Z}$ es un residuo cuadrático módulo p, por definición el polinomio $x^2 - \overline{m}$ tiene raíces en $\mathbf{Z}_p$, por lo que $\exists \overline{a} \in \mathbf{Z}_p$, $0 \leq a \leq p - 1$, tal que $\overline{a}^2 - \overline{m} = \overline{0}$, i.e., $\overline{m} = \overline{a}^2$. Para ver la inclusión deseada todo consiste en probar que $a \leq \frac{p-1}{2}$, y éso equivale a ver que, para cualquier $k > 0$, $(\overline{\frac{p-1}{2} + k})^2 \in \{\overline{0}, \overline{4}, \overline{9}, ..., (\overline{\frac{p-1}{2}})^2\}$

$$(\overline{\frac{p-1}{2} + k})^2 - (\overline{\frac{p-1}{2} - (k-1)})^2 = \overline{p(2k-1)} = \overline{0},$$

lo que implica que

$$(\overline{\frac{p-1}{2} + k})^2 = (\overline{\frac{p-1}{2} - (k-1)})^2 \in \{\overline{0}, \overline{4}, ..., (\overline{\frac{p-1}{2}})^2\}.$$

$[\supset]$ Trivial, $\forall a \in \{0, 1, 2, ..., \frac{p-1}{2}\}$, $x^2 - \overline{a}^2 = (x - \overline{a})(x + \overline{a})$. Por tanto, a^2 es residuo cuadrático módulo p. ♣

Ex. 189 *Para p primo, $p > 2$, demostrar que $x^2 - a \in \mathbf{Z}_p[x]$ tiene alguna raíz en $\mathbf{Z}_p$ si y sólo si $a^{\frac{p+1}{2}} = a$.*

$\equiv$

Para $a = 0$ la cosa es inmediata pues $0^{\frac{p+1}{2}} = 0$. Suponemos pues que $a \neq 0$.
$[\Rightarrow]$ Partimos de que $x^2 - a$ admite la raíz $b \in \mathbf{Z}_p$. Claramente, $b \neq 0$, es decir, $b \in \mathbf{Z}_p^*$, que recordemos es un grupo multiplicativo cíclico de orden $p - 1$. Así

$$a = b^2 \;\Rightarrow\; a^{\frac{p+1}{2}} = b^{p+1} = b^{p-1} \cdot b^2 = 1 \cdot b^2 = b^2 = a.$$

$[\Leftarrow]$ Suponiendo que $a^{\frac{p+1}{2}} = a$, entonces $1 = a^{\frac{p+1}{2} - 1} = a^{\frac{p-1}{2}}$. Como $\mathbf{Z}_p^*$ es un grupo mutiplicativo cíclico de orden $p - 1$, existe cierto $b \in \mathbf{Z}_p^*$ de modo que $\mathbf{Z}_p^* = \langle\, b \,\rangle$. Así, como $a \in \mathbf{Z}_p^*$, existe $k \in \{0, 1, ..., p - 1\}$ tal que $a = b^k$. Entonces

$$1 = a^{\frac{p-1}{2}} = b^{\frac{k(p-1)}{2}} \;\rightarrow\; p - 1 \mid \frac{k(p-1)}{2} \;\rightarrow\; 2 \mid k.$$

Sea $k = 2n$ y sea $c := b^n$. Entonces

$$c^2 \;=\; b^{2n} \;=\; b^k \;=\; a \;\rightarrow\; c^2 - a \;=\; 0.$$

Por tanto, c es una raíz del polinomio $x^2 - a$ en $\mathbf{Z}_p$. ♣

Ex. 190 *Especificar las condiciones que han de cumplir a y b para que la ecuación cuadrática $x^2 + ax + b = 0$ sea resoluble en $\mathbf{Z}_p$ (p primo).*

≡

Para $p = 2$, como $\mathbf{Z}_2 = \{0, 1\}$, queda claro que la única ecuación de segundo grado no resoluble es $x^2 + x + 1 = 0$. Es decir, en este caso, las ecuaciones $x^2 + 1 = 0$, $x^2 + x = 0$ y $x^2 = 0$ son las únicas resolubles en $\mathbf{Z}_2$.

Supongamos que $p > 2$. Veamos que la ecuación $x^2 + ax + b = 0$ es resoluble en $\mathbf{Z}_p$ si y sólo si $a^2 - 4b$ es un residuo cuadrático módulo p.

[$\Rightarrow$] Si la ecuación anterior tiene alguna solución, sea $c \in \mathbf{Z}_p$ tal que $c^2 + ac + b \;= 0$. Entonces

$$(2c + a)^2 \;-\; (a^2 - 4b) \;=\; 4(c^2 + ac + b) \;=\; 0 \;\rightarrow\; (2c + a)^2 \;=\; (a^2 - 4b).$$

Por tanto $x^2 - (a^2 - 4b)$ admite raices en $\mathbf{Z}_p$. Es decir, $a^2 - 4b$ es un residuo cuadrático módulo p.

[$\Leftarrow$] Si $a^2 - 4b$ es un residuo cuadrático módulo p, entonces existe $c \in \mathbf{Z}_p$ al que $c^2 = a^2 - 4b$. Consideremos $d := \frac{c-a}{2}$. Como $4b = a^2 - c^2 = (a + c)(a - c)$, se tiene que $4 \mid (c+a)(c-a) = (c-a+2a)(c-a)$, lo que implica que $2 \mid c - a$, i.e, $d \in \mathbf{Z}_p$. Finalmente veamos que d es raíz de $x^2 + ax + b$

$$d^2 + ad + b \;=\; \frac{(c-a)^2}{4} \;+\; a\frac{c-a}{2} \;+\; b \;=\; \frac{c^2 - a^2 + 4b}{4} \;=\; 0. \;\clubsuit$$

2.3. Extensiones de cuerpos

Ex. 191 *Sea $q(x) \in F[x]$. Definimos la siguiente relación binaria en $F[x]$*

$$f(x) \;\equiv\; g(x) \;(mod.q(x)) \quad\leftrightarrow\quad q(x) \mid f(x) - g(x).$$

a) Demostrar que se trata de una relación de equivalencia.
b) Si designamos mediante $F[x]/q(x)$ al conjunto cociente, demostrar que las operaciones

$$\overline{f(x)} \;+\; \overline{g(x)} \;=\; \overline{f(x) + g(x)}, \quad \overline{f(x)} \;\cdot\; \overline{g(x)} \;=\; \overline{f(x)g(x)}$$

están bien definidas en $F[x]/q(x)$.
c) Demostrar que $F[x]/q(x)$ con las operaciones anteriores es un cuerpo si y sólo si $q(x)$ es irreducible sobre F.

$\equiv$
a)
Reflexiva: $\forall f(x) \in F[x]$, es evidente que $f(x) \equiv f(x)\ (\text{mod}.q(x))$, pues $f(x) - f(x) = 0$ es divisible por $q(x)$.
Simétrica: $\forall f(x), g(x) \in F[x]$, suponiendo que $f(x) \equiv g(x)\ (\text{mod}.q(x))$, entonces

$$\exists h(x) \in F[x] \,/\, f(x) - g(x) = h(x)q(x) \rightarrow g(x) - f(x) = (-h(x))q(x) \rightarrow g(x) \equiv f(x)(mod.q(x)).$$

Transitiva: $\forall f(x), g(x), h(x) \in F[x]$, suponiendo que $f(x) \equiv g(x)$ y que $g(x) \equiv h(x)\ (mod.q(x))$, entonces

$$\left.\begin{array}{l} \exists r(x) \in F[x] \,/\, f(x) - g(x) = r(x)q(x) \\ \exists s(x) \in F[x] \,/\, g(x) - h(x) = s(x)q(x) \end{array}\right\}$$

$$\Rightarrow f(x) - h(x) = f(x) - g(x) + g(x) - h(x) = [r(x) + s(x)]q(x).$$

Luego $f(x) \equiv h(x)\ (mod.q(x))$.
b) Para ver que las operaciones suma y producto de clases están bien definidas, lo que hay que ver es que no dependen del representante elegido. Así, sean $\overline{f(x)} = \overline{r(x)}$ y $\overline{g(x)} = \overline{s(x)}$. Entonces existen polinomios $u(x), v(x) \in F[x]$ tales que $f(x) - r(x) = u(x)q(x)$ y $g(x) - s(x) = v(x)q(x)$. Así

$$\left.\begin{array}{l} f(x) + g(x) = r(x) + s(x) + [u(x) + v(x)]q(x) \;\rightarrow\; \overline{f(x) + g(x)} = \overline{r(x) + s(x)} \\ f(x)g(x) = r(x)s(x) + q(x)[r(x)v(x) + s(x)u(x)] \;\rightarrow\; \overline{f(x)g(x)} = \overline{r(x)s(x)} \end{array}\right\}$$

$$\Rightarrow \left\{\begin{array}{l} \overline{f(x)} + \overline{g(x)} = \overline{r(x)} + \overline{s(x)} \\ \overline{f(x)} \cdot \overline{g(x)} = \overline{r(x)} \cdot \overline{s(x)}. \end{array}\right.$$

c) [$\Rightarrow$] Supongamos que $F[x]/q(x)$ es un cuerpo. Sea $q(x) = f(x)g(x)$, con $f(x), g(x) \in F[x]$. Entonces $\overline{0} = \overline{f(x)} \cdot \overline{g(x)}$ en $F[x]/q(x)$ y, al ser un cuerpo, ello implica que alguna de las dos clases ha de ser la nula. Es decir

$$\left.\begin{array}{l} \text{Si } \overline{f(x)} = \overline{0} \rightarrow\ q(x) \mid f(x) \ \rightarrow grado(f(x)) = grado(q(x)),\ grado(g(x)) = 0 \\ \text{Si } \overline{g(x)} = \overline{0} \rightarrow\ q(x) \mid g(x) \ \rightarrow grado(g(x)) = grado(q(x)),\ grado(f(x)) = 0 \end{array}\right\}$$

$$\Rightarrow\ q(x) \text{ irred. sobre } F.$$

[$\Leftarrow$] Como es mecánico verificar que $F[x]/q(x)$ cumple todos los axiomas de la definición de cuerpo, tan sólo nos limitaremos a demostrar que todo elemento no nulo admite inverso. Así, sea $\overline{f(x)} \in F[x]/q(x) \setminus \{\overline{0}\}$. Como, por hipótesis, $q(x)$ es irreducible sobre F, $mcd(f(x), q(x)) = 1$ y, del Lema de Bezout, existen dos polomios $u(x), v(x) \in F[x]$ tales que $1 = u(x)f(x) + v(x)q(x)$. Por tanto, $q(x) \mid 1 - u(x)f(x)$, de donde $\overline{1 - u(x)f(x)} = \overline{0}$, i.e.,

$$\overline{1} \;=\; \overline{u(x)f(x)} \;=\; \overline{u(x)} \cdot \overline{f(x)} \;\Rightarrow\; \overline{f(x)}^{-1} \;=\; \overline{u(x)}. \;\clubsuit$$

Ex. 192 *Sea $q(x)$ irreducible sobre F.*

1) Demostrar que $E := F[x]/q(x)$ es una extensión finita de F tal que $[E : F] = grado(q(x))$.

2) Considerando que $q(x) \in E[x]$, demostrar que $q(x)$ tiene una raíz en E.

$\equiv$

Antes de ponernos a resolverlo, notar la grandiosidad de este ejercicio. Nos dice que, dado un polinomio irreducible sobre un cuerpo F, siempre se puede encontrar una extensión del cuerpo (incluso algebraica) en donde el polinomio irreducible inicial ahora ya es reducible, ya que admite raíces en el cuerpo extensión. Una extensión E de un cuerpo F se dice que es una extensión algebraica siempre que $\forall \omega \in E$, $\exists f(x) \in F[x]$ tal que $f(\omega) = 0$. Por ejemplo, $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ : \ a, b \in \mathbf{Q}\}$ es una extensión algebraica de $\mathbf{Q}$, ya que todo elemento de $\mathbf{Q}(\sqrt{2})$ es raíz de un polinmio de $\mathbf{Q}[x]$, de hecho, el único no trivial es $\sqrt{2}$ que es raíz de $x^2 - 2 \in \mathbf{Q}[x]$. Ya que estamos, se dice que una extensión E del cuerpo F es una extensión finita siempre que, considerando E como espacio vectorial sobre F, la dimensión $[E : F]$ es finita. Conviene saber que toda extensión finita es algebraica. También es importante saber que el cuerpo de los números complejos $\mathbf{C}$ es una extensión finita del cuerpo de los números reales $\mathbf{R}$, ya que $\mathbf{C} = \{a + bi \ : \ a, b \in \mathbf{R}\}$ cumple que $[\mathbf{C} : \mathbf{R}] = 2$. Sí, ... $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}]$ también vale 2, o sea, $\mathbf{Q}(\sqrt{2})$ es una extensión finita (por tanto algebraica, como ya vimos) de $\mathbf{Q}$.

1) Ya vimos en el ejercicio previo que, como $q(x)$ es irreducible sobre F, $E := F[x]/q(x)$ es un cuerpo. Ya que estrictamente hablando F no está contenido en E, lo que hacemos es ver que F es isomorfo (como cuerpo) a un subcuerpo de E. Para ello, definimos

$$\begin{array}{rccl} \varphi & : & F & \longrightarrow & E \\ & & a & \to & \varphi(a) := \overline{a} = \ a \ + \ q(x)F[x]. \end{array}$$

φ homomorfismo de cuerpos: Dados $a, b \in F$

$$\varphi(a + b) = \overline{a + b} = (a + b) + q(x)F[x] = (a + q(x)F[x]) + (b + q(x)F[x]) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \overline{ab} = (ab) + q(x)F[x] = (a + q(x)F[x])(b + q(x)F[x]) = \varphi(a)\varphi(b).$$

φ inyectiva: Si $a \in Ker(\varphi)$

$$\overline{0} \ = \ \varphi(a) \ = \ \overline{a} \to \ q(x) \mid a \ \overset{(grado(q(x))>0)}{\to} \ a \ = \ 0.$$

Por comodidad, tradicionalmente se sigue representando como F al subcuerpo imagen $\varphi(F)$ de E. Sea $grado(q(x)) = n$ y veamos que $[E : F] = n$. Para verlo hay que encontrar una base de E sobre F que conste de n vectores. Así, sea

$$B \ := \ \{ \ \overline{1}, \ \overline{x}, \ \overline{x^2}, \ ..., \ \overline{x^{n-1}} \ \}.$$

Claramente, $B \subset E$. Veamos que B es base de E (considerado como espacio vectorial sobre F).

B linealmente independiente: Sean $c_0, c_1, ..., c_{n-1} \in F$ tales que

$$c_0\overline{1} + c_1\overline{x} + c_2\overline{x^2} + ... + c_{n-1}\overline{x^{n-1}} = \overline{0}.$$

Entonces, como $grado(q(x)) = n$,

$$\overline{0} = \overline{c_0 + c_1x + ... + c_{n-1}x^{n-1}} \Rightarrow q(x) \mid c_0 + c_1x + ... + c_{n-1}x^{n-1} \Rightarrow c_0 = c_1 = ... = c_{n-1} = 0.$$

B sistema generador de E: Dada $\overline{f(x)} \in E$, aplicando el algoritmo de la división polinómica, existsn $g(x), r(x) \in F[x]$ tales que

$$f(x) = g(x)q(x) + r(x), \quad grado(r(x)) < n, \ ó, \ r(x) = 0.$$

Supongamos que $r(x) = a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1}$, donde algunos coeficientes $a_0, a_1, ..., a_{n-1}$ (incluso todos) puede ser 0. Entonces, de la igualdad anterior (prueba de la división), trabajando en$E = F[x]/q(x)$, tenemos

$$\overline{f(x)} = \overline{g(x)q(x) + r(x)} = \overline{0} + \overline{r(x)} = \overline{a_0 + a_1x + ... + a_{n-1}x^{n-1}}$$

$$= a_0\overline{1} + a_1\overline{x} + ... + a_{n-1}\overline{x^{n-1}}.$$

2) Sea $q(x) = \alpha_0 + \alpha_1x + ... + \alpha_nx^n$, $\alpha_0, \alpha_1, ..., \alpha_n \in F$. Como $F \subset E$ (después de la identificación antes explicada), tenemos que $q(x) \in F[x] \subset E[x]$ y podemos escribir

$$q(x) = \overline{\alpha_0} + \overline{\alpha_1}\, x + ... \overline{\alpha_n}\, x^n.$$

Con un poco de abstracción se comprende enseguida que $\omega := \overline{x}$ es un elemento de E. Además

$$q(\omega) = \overline{\alpha_0} + \overline{\alpha_1}\, \omega + ... \overline{\alpha_n}\, \omega^n = \overline{\alpha_0} + \overline{\alpha_1}\, \overline{x} + ... \overline{\alpha_n}\, \overline{x}^n$$

$$= \overline{\alpha_0 + \alpha_1x + ... + \alpha_nx^n} = \overline{q(x)} = \overline{0}.$$

Hemos demostrado que $\omega = \overline{x} \in E$ es raíz de $q(x)$. ♣

Ex. 193 *Demostrar que el cuerpo* $\mathbf{R}[x]/(x^2 + 1)$ *es isomorfo a* $\mathbf{C}$.

≡

Este resultado demuestra que $\mathbf{C}$ es una extensión finita de $\mathbf{R}$ de grado 2, ya que, del ejercicio anterior $\mathbf{R}[x]/(x^2 + 1)$ es una extensión de $\mathbf{R}$ tal que $[\mathbf{R}[x]/(x^2 + 1) : \mathbf{R}] = grado(x^2 + 1) = 2$. Notar que $x^2 + 1$ es irreducible sobre $\mathbf{R}$.

Como se debe hacer, todo se reduce a definir un isomorfismo de cuerpos entre $\mathbf{R}[x]/(x^2 + 1)$ y $\mathbf{C}$, o al revés.

$$\begin{array}{rccl} \varphi & : & \mathbf{C} & \longrightarrow \mathbf{R}[x]/(x^2 + 1) \\ & & a + b\mathbf{i} & \to \varphi(a + b\mathbf{i}) := \overline{a + bx}. \end{array}$$

φ homomorfismo de cuerpos: Dados los complejos $a+b\mathbf{i},\ c+d\mathbf{i}$

$$\varphi[(a+b\mathbf{i})+(c+d\mathbf{i})]=\varphi[(a+c)+(b+d)\mathbf{i}]=\overline{(a+c)+(b+d)x}$$
$$\varphi(a+b\mathbf{i})+\varphi(c+d\mathbf{i})=\overline{a+bx}+\overline{c+dx}$$
$$\varphi[(a+b\mathbf{i})(c+d\mathbf{i})]=\varphi[(ac-bd)+(ad+bc)\mathbf{i}]=\overline{(ac-bd)+(ad+bc)x}$$
$$\varphi(a+b\mathbf{i})\varphi(c+d\mathbf{i})=\overline{a+bx}\cdot\overline{c+dx}=\overline{ac+(ad+bc)x+bcx^2}$$
$$=\overline{bd(x^2+1)+(ad+bc)x+(ac-bd)}=\overline{(ad+bc)x+(ac-bd)}.$$

φ inyectiva: Si $a+b\mathbf{i}\in Ker(\varphi)$, entonces

$$\overline{0}\ =\ \varphi(a+b\mathbf{i})\ =\ \overline{a+bx}\ \rightarrow\ (x^2+1)\mid(a+bx)\ \rightarrow\ a=b=0.$$

φ sobre: Dada $\overline{f(x)}\in\mathbf{R}[x]/(x^2+1)$, dividiendo por el módulo x^2+1, existen $c(x),r(x)\in\mathbf{R}[x]$ tales que $f(x)=c(x)(x^2+1)+r(x),\ \ r(x)=0$ ó $grado(r(x))<2$.

$$\text{Si } r(x)=0\ \rightarrow\ \overline{f(x)}=\overline{0}\ \rightarrow\ \varphi(0)=\overline{f(x)}$$
$$\text{Si } grado(r(x))<2\ \rightarrow\ \exists a,b\in\mathbf{R}\ /\ r(x)=a+bx$$
$$\rightarrow\ \varphi(a+b\mathbf{i})=\overline{a+bx}=\overline{r(x)}=\overline{f(x)}.\ \clubsuit$$

Ex. 194 *Demostrar que el cuerpo* $\mathbf{Q}[x]/(x^2-2)$ *es isomorfo a* $\mathbf{Q}(\sqrt{2})$.

$\equiv$

Análogamente a lo hecho en el anterior ejercicio, ésto demuestra que $\mathbf{Q}(\sqrt{2})$ es una extensión finita de $\mathbf{Q}$ de grado 2. Como antes, vamos a definir un isomorfismo de cuerpos.

$$\begin{array}{rccl}\varphi & : & \mathbf{Q}(\sqrt{2}) & \longrightarrow\ \mathbf{Q}[x]/(x^2-2)\\ & & a+b\sqrt{2} & \rightarrow\ \varphi(a+b\sqrt{2}):=\overline{a+bx}.\end{array}$$

φ homomorfismo de cuerpos: Dados los números $a+b\sqrt{2},\ c+d\sqrt{2}$

$$\varphi[(a+b\sqrt{2})+(c+d\sqrt{2})]=\varphi[(a+c)+(b+d)\sqrt{2}]=\overline{(a+c)+(b+d)x}$$
$$\varphi(a+b\sqrt{2})+\varphi(c+d\sqrt{2})=\overline{a+bx}+\overline{c+dx}$$
$$\varphi[(a+b\sqrt{2})(c+d\sqrt{2})]=\varphi[(ac+2bd)+(ad+bc)\sqrt{2}]=\overline{(ac+2bd)+(ad+bc)x}$$
$$\varphi(a+b\sqrt{2})\varphi(c+d\sqrt{2})=\overline{a+bx}\cdot\overline{c+dx}=\overline{ac+(ad+bc)x+bcx^2}$$
$$=\overline{bd(x^2-2)+(ad+bc)x+(ac+2bd)}=\overline{(ad+bc)x+(ac+2bd)}.$$

φ inyectiva: Si $a+b\sqrt{2}\in Ker(\varphi)$, entonces

$$\overline{0}\ =\ \varphi(a+b\sqrt{2})\ =\ \overline{a+bx}\ \rightarrow\ (x^2-2)\mid(a+bx)\ \rightarrow\ a=b=0.$$

φ sobre: Dada $\overline{f(x)}\in\mathbf{Q}[x]/(x^2-2)$, dividiendo por el módulo x^2-2, existen $c(x),r(x)\in\mathbf{Q}[x]$ tales que $f(x)=c(x)(x^2-2)+r(x),\ \ r(x)=0$ ó $grado(r(x))<2$.

$$\text{Si } r(x)=0\ \rightarrow\ \overline{f(x)}=\overline{0}\ \rightarrow\ \varphi(0)=\overline{f(x)}$$
$$\text{Si } grado(r(x))<2\ \rightarrow\ \exists a,b\in\mathbf{R}\ /\ r(x)=a+bx$$
$$\rightarrow\ \varphi(a+b\sqrt{2})=\overline{a+bx}=\overline{r(x)}=\overline{f(x)}.\ \clubsuit$$

Ex. 195 *Demostrar el Teorema de Kronecker: Dado $f(x) \in F[x]$, existe una extensión finita E de F tal que $f(x)$ se descompone totalmente en E.*

$\equiv$

De un ejercicio anterior sabemos que todo polinomio $f(x)$ admite un divisor irreducible sobre F. Por tanto, todo consiste en ver que si $f(x)$ es un polinomio irreducible sobre F existe una extensión finita E de F en donde $f(x)$ se descompone totalmente. Del ejercicio 191, $E_1 := F[x]/f(x)$ es una extensión finita de F tal que $f(x)$ tiene una raíz en E_1. Sea $\omega_1 \in E_1$ dicha raíz, entonces $f(x) = (x - \omega_1) \cdot f_1(x)$, $f_1(x) \in E_1[x]$. Si $f_1(x)$ es reducible sobre E_1, se factoriza; si es irreducible, $E_2 := E_1[x]/f_1(x)$ es una extensión finita de E_1 tal que $f_1(x)$ tiene una raíz en E_1. Llamando como antes ω_2 a dicha raíz, se tiene que $f_1(x) = (x - \omega_2)f_2(x)$. Procediendo de este modo una cantidad finita de veces (menor o igual que el grado de $f(x)$) obtenemos una cadena de extensiones $F \subset E_1 \subset E_2 \subset ... \subset E_k$ y unos elementos $\omega_i \in E_i$, $1 \leq i \leq k$, de modo que

$$f(x) \;=\; (x - \omega_1)(x - \omega_2)...(x - \omega_k), \quad \omega_1, \omega_2, ..., \omega_k \in E_k.$$

Por tanto E_k es una extensión finita de F en donde $f(x)$ factoriza totalmente. ♣

Ex. 196 *Dado p primo, $p > 2$, construir un cuerpo con p^2 elementos.*

$\equiv$

De un ejercicio anterior, ya que $p > 2$, sabemos que los residuos cuadráticos módulo p de $\mathbf{Z}_p$ son

$$0,\ 1,\ 4,\ 9,\ ...\ (\frac{p-1}{2})^2\ .$$

Sea $a \in \mathbf{Z}_p \setminus \{0, 1, 4, ..., (\frac{p-1}{2})^2\}$, i.e., $a \in \mathbf{Z}_p$ no es un residuo cuadrático módulo p. Veamos que $F := \mathbf{Z}_p[x]/(x^2 - a)$ es un cuerpo con p^2 elementos. Para empezar, F es un cuerpo ya que, al no ser a residuo cuadrático módulo p, $x^2 - a$ es irreducible sobre $\mathbf{Z}_p$. Además, F es una extensión de $\mathbf{Z}_p$ tal que $[F : \mathbf{Z}_p] = grado(x^2 - a) = 2$. Por tanto, F puede considerarse como un espacio vectorial sobre $\mathbf{Z}_p$ de dimensión 2. Es fácil verificar que F es isomorfo (como espacio vectorial) a $\mathbf{Z}_p \times \mathbf{Z}_p$, de donde obtenemos que

$$card(F) \;=\; card(\mathbf{Z}_p \times \mathbf{Z}_p) \;=\; card(\mathbf{Z}_p)^2 \;=\; p^2\ . \clubsuit$$

Ex. 197 *Sea p primo. Demostrar que el polinomio $\Phi_p(x) = 1 + x + x^2 + ... + x^{p-1}$ es irreducible sobre $\mathbf{Q}$.*

$\equiv$

Primero manipulamos el polinomio dado. Sea $\psi_p(x) := \Phi_p(x + 1)$. Sabemos que la irrducibilidad de $\Phi(x)$ es equivalente a la de $\psi_p(x)$. Así, vamos a desarrollar $\psi_p(x)$ y después le aplicaremos el criterio de Eisenstein.

$$\psi_p(x) \;=\; \Phi_p(x+1) \;=\; 1 + (x+1) + (x+1)^2 + ... + (x+1)^{p-1} \overset{(P.G.,r=x+1)}{=} \frac{(x+1)^p - 1}{(x+1) - 1}$$

$$= \frac{x^p + px^{p-1} + \frac{p(p-1)}{2}x^{p-2} + ... + px + 1 - 1}{x}$$

$$= x^{p-1} + px^{p-2} + \frac{p(p-1)}{2}x^{p-3} + ... + p.$$

Aplicando el criterio de Eisenstein

$$a_0 = p, \quad a_1 = \frac{p(p-1)}{2}, \quad a_2 = \frac{p(p-1)(p-2)}{6}, \quad ..., \quad a_{p-2} = p, \quad a_{p-1} = 1.$$

Verificando las tres condiciones del criterio

$$\begin{array}{l} p \mid a_i, \quad 0 \leq i \leq p-2 \\ p \not\mid a_{p-1} \\ p^2 \not\mid a_0. \end{array}$$

Por tanto, $\psi_p(x)$, y también $\Phi_p(x)$, es irreducible sobre $\mathbf{Q}$. ♣

Ex. 198 *Sea $F(x)$ el cuerpo de las fracciones polinómicas asociado a $F[x]$, es decir*

$$F(x) = \{ \frac{f(x)}{g(x)} : f(x), g(x) \in F[x], \ g(x) \neq 0 \}.$$

Sea $\Phi(X) = f_0(x) + f_1(x)X + f_2(x)X^2 + ... + f_n(x)X^n \in F(x)[X]$, con coeficientes $f_0(x), f_1(x), ..., f_n(x) \in F[x]$. Demostrar que las siguientes tres condiciones son suficientes para poder afirmar que $\Phi(X)$ es irreducible sobre $F(x)$ (se trata de un análogo al criterio de Eisenstein):

Condición 1: x divide a cada coeficiente $f_0(x), f_1(x), ..., f_{n-1}(x)$.
Condición 2: x no divide a $f_n(x)$.
Condición 3: x^2 no divide a $f_0(x)$.

≡

Razonando por reducción al absurdo, supongamos que $\Phi(X)$ fuese reducible sobre $F(x)$. Entonces existen $\varphi(X), \psi(X) \in F(x)[X]$ tales que $\Phi(X) = \varphi(X)\psi(X)$. Supongamos que

$$\begin{array}{l} \varphi(X) = g_0(x) + g_1(x)X + ... + g_r(x)X^r \\ \psi(X) = h_0(x) + h_1(x)X + ... + h_s(x)X^s. \end{array}$$

Entonces

$$\left.\begin{array}{l} f_0(x) = g_0(x)h_0(x) \\ f_1(x) = g_0(x)h_1(x) + g_1(x)h_0(x) \\ f_2(x) = g_0(x)h_2(x) + g_1(x)h_1(x) + g_2(x)h_0(x) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_n(x) = g_0(x)h_n(x) + g_1(x)h_{n-1}(x) + ... + g_n(x)h_0(x) \end{array}\right\} \text{ donde } \left\{\begin{array}{l} 0 = g_i(x), \ \forall i > r \\ 0 = h_j(x) \forall j > s. \end{array}\right.$$

De la Condición 1, como $x \mid f_0(x) = g_0(x)h_0(x)$, se tiene que $x \mid g_0(x)$ ó $x \mid h_0(x)$. Supongamos que $x \mid g_0(x)$ (análogo en el otro caso), entonces $x \not\mid h_0(x)$, de lo contrario

$x^2 \mid f_0(x)$, lo que contradice la Condición 3. Como $x \mid f_1(x)$, ello implica que $x \mid g_1(x)h_0(x)$. Pero, como $x \not| h_0(x)$, tenemos que $x \mid g_1(x)$. Procediendo de esta forma, obtenemos que

$$x \mid g_0(x), \quad x \mid g_1(x), \quad ...., \quad x \mid g_r(x).$$

Ello implica que x es divisor de todos los coeficientes $f_0(x), f_1(x), ..., f_n(x)$. Absurdo, ya que se contradice la Condición 2. ♣

Ex. 199 *Sea α un número algebraico. Demostrar que, para cualquier $r \in \mathbf{Q}$, los números $r+\alpha$ y $r\alpha$ también son algebraicos.*

≡

Recordemos que un número real α es algebraico siempre que existe un polinomio $f(x) \in \mathbf{Q}[x]$ tal que $f(\alpha) = 0$, es decir, los números algebraicos son las raíces de polinomios de $\mathbf{Q}[x]$ (observar que sería equivalente dar la definición en términos de $\mathbf{Z}[x]$). Así, para ver que $r+\alpha$ es algebraico, sea $f(x) \in \mathbf{Q}[x]$ tal que $f(\alpha) = 0$. Tomando $g(x) := f(x-r)$, como $r \in \mathbf{Q}$, está claro que $g(x) \in \mathbf{Q}[x]$ y $g(r+\alpha) = f(r+\alpha-r) = f(\alpha) = 0$.

Para ver que $r\alpha$ es algebraico, sea $h(x) := f(\frac{x}{r})$ (suponemos $r \neq 0$, sino, obvio), como $r \in \mathbf{Q}$, está claro que $h(x) \in \mathbf{Q}[x]$ y $h(r\alpha) = f(\frac{r\alpha}{r}) = f(\alpha) = 0$. ♣

Ex. 200 *Demostrar que, para cualquier $r \in \mathbf{Q}$, $\cos r\pi$ es algebraico.*

≡

Sea $r = \frac{p}{q}$, $p, q \in \mathbf{Z}$, $q > 0$. Aplicando la fórmula de De Moivre

$$(\cos\frac{p\pi}{q} + \mathbf{i}\ \sin\frac{p\pi}{q})^{2q} \ = \ \cos 2p\pi \ + \ \mathbf{i}\ \sin 2p\pi \ = \ 1.$$

Pero, por otra parte, llamando (comodidad) $a := \cos\frac{p\pi}{q}$, $b := \mathbf{i}\ \sin\frac{p\pi}{q}$, tenemos

$$(a+b)^{2q} \ = \ \binom{2q}{0} a^{2q} + \binom{2q}{1} a^{2q-1}b + \binom{2q}{2} a^{2q-2}b^2 + ... + \binom{2q}{2q} b^{2q}.$$

Pero, como

$$\begin{aligned} b^2 \ &= \ (\mathbf{i}\ \sin\tfrac{p\pi}{q})^2 = a^2 - 1 \\ b^4 \ &= = \ (a^2-1)^2 \\ &..... \\ &..... \\ b^{2q} \ &= = \ (a^2-1)^q, \end{aligned}$$

se deduce que

$$1 \ = \ Re[(a+b)^{2q}] \ = \ \binom{2q}{0} a^{2q} + \binom{2q}{2} a^{2q-2}b^2 \binom{2q}{4} a^{2q-4}b^4 + ... + \binom{2q}{2q} b^{2q}$$

$$= \ \binom{2q}{0} a^{2q} + \binom{2q}{2} a^{2q-2}(a^2-1) \binom{2q}{4} a^{2q-4}(a^2-1)^2 + ... + \binom{2q}{2q} (a^2-1)^q.$$

Llamando

$$f(x) := \binom{2q}{0} x^{2q} + \binom{2q}{2} x^{2q-2}(x^2-1) \binom{2q}{4} x^{2q-4}(x^2-1)^2 + \ldots + \binom{2q}{2q} (x^2-1)^q - 1$$

tenemos que $f(x) \in \mathbf{Q}[x]$ y

$$f(\cos r\pi) = f(\cos \frac{p\pi}{q}) = f(a) = 0. \clubsuit$$

Ex. 201 *Sea $f(x) \in F[x]$ un polinomio irreducible. Sea E una extensión de F en la que $f(x)$ tiene una raíz $\alpha \in E$. Demostrar que $f(x)$ es un polinomio mínimo de α sobre F.*

≡

Recordemos primero que, en general, un polinomio $f(x) \in F[x]$, que admite una raíz α en una extensión E de F, es un polinomio mínimo de α sobre F siempre que el grado de $f(x)$ sea el menor de todos los grados de los polinomios de $F[x]$ que tienen α como raíz. Así, sea $g(x) \in F[x]$ un polinomio mínimo de α sobre F, cuya existencia está garantizada. Dividiendo $f(x)$ por $g(x)$, existen $c(x), r(x) \in F[x]$ tales que

$$f(x) = c(x)g(x) + r(x), \quad grado(r(x)) < grado(g(x)).$$

Entonces

$$0 = f(\alpha) = c(\alpha)g(\alpha) + r(\alpha) = r(\alpha) \Rightarrow r(x) = 0,$$

de lo contrario se contradice que $g(x)$ es polinomio mínimo de α sobre F. Por tanto, $f(x) = c(x)g(x)$. Pero, al ser $f(x)$ irreducible sobre F y puesto que $grado(g(x)) > 0$, ello implica que $c(x)$ es constante. Es decir, $grado(f(x)) = grado(g(x))$, por lo que $f(x)$ es un polinomio mínimo de α sobre F. $\clubsuit$

Ex. 202 *Sea $F \subset E \subset D$ una torre de cuerpos. Sea $g(x)$ un polinomio mínimo de $\alpha \in D$ sobre E. Sea ahora $f(x)$ un polinomio mínimo de α sobre F. Considerando $f(x), g(x) \in E[x]$, demostrar que $g(x) \mid f(x)$.*

≡

Observar que este ejercicio nos dice que los polinomios mínimos de una misma raíz están ordenados por divisibilidad inversamente según sobre la altura del piso de la torre sobre el que está referido el polinomio.

Primero, notemos que, como $\alpha \in D$, $F \subset E \subset D$ y $g(x) \in E[x]$, $f(x) \in F[x] \subset E[x]$ el enunciado tiene sentido. Entonces, todo resulta más claro. Para empezar $g(x)$ es polinomio mínimo de α sobre E, lo que significa que $g(x) \in E[x]$, $g(\alpha) = 0$ y que $grado(g(x))$ es el menor de los grados de los polinomios de $E[x]$ que admiten α como raíz. Así, como $f(x) \in F[x] \subset E[x]$ y, al ser polinomio mínimo de α, $f(\alpha) = 0$, tenemos que $grado(f(x)) \geq grado(g(x))$. Dividiendo $f(x)$ por $g(x)$ en $E[x]$

$$f(x) = c(x)g(x) + r(x), \quad c(x), r(x) \in E[x], \quad grado(r(x)) < grado(g(x)).$$

Como hicimos en el ejercicio previo, se deduce que $r(x) = 0$, de donde $g(x) \mid f(x)$. $\clubsuit$

Ex. 203 *Hallar los polinomios mínimos sobre* $\mathbf{Q}$, *y sobre* $\mathbf{Q}(\sqrt{2})$, *de los números* $\sqrt{2}+\sqrt{3}$ *e* $\mathbf{i}\cdot\sqrt{2}$.

≡

Primero lo hacemos sobre $\mathbf{Q}$.

$$(x-\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3}) = x^2-(\sqrt{2}+\sqrt{3})^2 = x^2-5-2\sqrt{6}$$
$$(x^2-5-2\sqrt{6})(x^2-5+2\sqrt{6}) = (x^2-5)^2-24 = x^4-10x^2+1.$$

El polinomio $x^4-10x^2+1 \in \mathbf{Q}[x]$ es irreducible sobre $\mathbf{Q}$ (al ser bicuadrado, su discriminante vale $100-4=96=16\cdot 6$, de lo que, como la raíz cuadrada del discriminante es $4\sqrt{6}$, no tiene raíces en $\mathbf{Q}$). Aplicando un ejercicio anterior, se tiene que x^4-10x^2+1 es un polinomio mínimo de $\sqrt{2}+\sqrt{3}$ sobre $\mathbf{Q}$.

Para el número $\mathbf{i}\sqrt{2}$, el polinomio $x^2+2 \in \mathbf{Q}[x]$ es un polinomio mínimo sobre $\mathbf{Q}$, ya que $\mathbf{i}\sqrt{2}$ es raíz de dicho polinomio y éste es claramente irreducible sobre $\mathbf{Q}$, luego se trata de un polinomio mínimo de dicho número sobre $\mathbf{Q}$.

Ahora hacemos lo mismo pero sobre el cuerpo $\mathbf{Q}(\sqrt{2})$.

Haciendo cálculos

$$(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3}) = (x-\sqrt{2})^2-3 = x^2-2\sqrt{2}x-1.$$

El polinomio $x^2-2\sqrt{2}x-1 \in \mathbf{Q}(\sqrt{2})[x]$ es irreducible sobre $\mathbf{Q}(\sqrt{2})$, ya que sus raíces son

$$\frac{2\sqrt{2}\pm\sqrt{8+4}}{2} = \frac{2\sqrt{2}\pm 2\sqrt{3}}{2} \notin \mathbf{Q}(\sqrt{2}).$$

Por tanto, $x^2-2\sqrt{2}x-1$ es un polinomio mínimo del número $\sqrt{2}+\sqrt{3}$ sobre $\mathbf{Q}(\sqrt{2})$.

Finalmente, el polinomio $x^2+2 \in \mathbf{Q}(\sqrt{2})[x]$ es claramente un polinomio mínimo del número $\mathbf{i}\sqrt{2}$, ya que sigue siendo irreducible sobre $\mathbf{Q}(\sqrt{2})$, puesto que sus únicas raíces $\pm\mathbf{i}\sqrt{2}$ no pertenecen a $\mathbf{Q}(\sqrt{2})$. ♣

Ex. 204 *Sea* E *una extensión de* F. *Sea* $\alpha \in E$ *algebraico sobre* F. *Demostrar que, si* $f(x)$ *es un polinomio mínimo de* α *sobre* F, *entonces* $F(\alpha)$ *es isomorfo a* $F[x]/(f(x))$.

≡

Definimos

$$\varphi : F[x]/(f(x)) \longrightarrow F(\alpha)$$
$$\overline{g(x)} \to \varphi(\overline{g(x)}) := g(\alpha).$$

φ bien definida: Si $\overline{g(x)} = \overline{h(x)}$, etonces existe un polinomio $p(x) \in F[x]$ tal que $g(x)-h(x) = p(x)f(x)$. Entonces, como $f(\alpha)=0$,

$$\varphi(\overline{g(x)}) = g(\alpha) = h(\alpha)+p(\alpha)f(\alpha) = h(\alpha) = \varphi(\overline{h(x)}).$$

φ homomorfismo de cuerpos: Si $\overline{g(x)}, \overline{h(x)} \in F[x]/(f(x))$

$$\varphi(\overline{g(x)}+\overline{h(x)}) = \varphi(\overline{g(x)+h(x)}) = g(\alpha)+h(\alpha) = \varphi(\overline{g(x)})+\varphi(\overline{h(x)})$$
$$\varphi(\overline{g(x)h(x)}) = \varphi(\overline{g(x)h(x)}) = g(\alpha)h(\alpha) = \varphi(\overline{g(x)})\varphi(\overline{h(x)}).$$

φ inyectiva: Si $\overline{g(x)} \in Ker(\varphi)$, entonces

$$0 = \varphi(\overline{g(x)}) = g(\alpha) \overset{(f(x) \text{ minimo})}{\Rightarrow} f(x) \mid g(x) \Rightarrow \overline{g(x)} = \overline{0}.$$

φ sobre: Si $\beta \in F(\alpha)$, entonces, por definición del cuerpo $F(\alpha)$, si $grado(f(x)) = n$, sabemos que $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ es una base de $F(\alpha)$ sobre F. Así, existen $c_0, c_1, ..., c_{n-1} \in F$ de modo que $\beta = c_0 + c_1\alpha + ... + c_{n-1}\alpha^{n-1}$. Considerando el polinomio $g(x) := c_0 + c_1x + ... + c_{n-1}x^{n-1} \in F[x]$, tenemos que

$$\varphi(\overline{g(x)}) = g(\alpha) = c_0 + c_1\alpha + ... + c_{n-1}\alpha^{n-1} = \beta. \clubsuit$$

Ex. 205 *Sea E una extensión de F. Sean $\alpha, \beta \in E$ algebraicos sobre F. Es evidente que α es algebraico sobre $F(\beta)$ y que β es algebraico sobre $F(\alpha)$. Sean $F(\alpha, \beta) = F(\alpha)(\beta)$ y $F(\beta, \alpha) = F(\beta)(\alpha)$.*

1) Demostrar que $F(\alpha, \beta) = F(\beta, \alpha)$.

2) Qué se puede afirmar de $[F(\alpha, \beta) : F]$?

$\equiv$

1) Recordemos que $F(\alpha)$ es el menor cuerpo que contiene a F y a α. Así

$$\left.\begin{array}{l} F \subset F(\beta) \subset F(\beta)(\alpha) = F(\beta, \alpha) \\ \alpha \in F(\beta)(\alpha) = F(\beta, \alpha) \\ \beta \in F(\beta) \subset F(\beta)(\alpha) = F(\beta, \alpha) \end{array}\right\} \rightarrow F(\alpha) \subset F(\beta, \alpha) \Bigg\}$$

$$\Rightarrow F(\alpha, \beta) = F(\alpha)(\beta) \subset F(\beta, \alpha).$$

La inclusión recíproca es análoga.

2) Sean $f(x)$ y $g(x)$ polinomios mínimos de α y de β, respectivamente, sobre F. Sean $grado(f(x)) = n$ y $grado(g(x)) = m$. Sabemos que $[F(\alpha) : F] \leq n$ y $[F(\beta) : F] \leq m$. En un problema anterior vimos que, si $h(x)$ es un polinomio mínimo de β sobre $F(\alpha) \supset F$, entonces $h(x) \mid g(x)$. Así

$$[F(\alpha)(\beta) : F(\alpha)] \leq grado(h(x)) \leq grado(g(x)) = m.$$

Por tanto

$$[F(\alpha, \beta) : F] = [F(\alpha)(\beta) : F(\alpha)] \cdot [F(\alpha) : F] \leq m \cdot n \ . \clubsuit$$

Ex. 206 *Sea $f(x) \in F[x]$ tal que $grado(f(x)) = n$. Sea E una extensión de F tal que contiene a las n raíces $\alpha_1, \alpha_2, ..., \alpha_n$ de $f(x)$. Se representa por $F(\alpha_1, \alpha_2, ..., \alpha_n)$ al menor subcuerpo de E que contiene a F y a $\alpha_1, \alpha_2, ..., \alpha_n$. Este cuerpo $F(\alpha_1, \alpha_2, ..., \alpha_n)$ recibe el nombre de cuerpo raíz, o, cuerpo de descomposición de $f(x)$ en E. Demostrar que $[F(\alpha_1, \alpha_2, ..., \alpha_n) : F] \leq n!$.*

$\equiv$

En $E[x]$

$$f(x) = (x - \alpha_1)(x - \alpha_2) ... (x - \alpha_n).$$

Claramente, $F(\alpha_1, \alpha_2, ..., \alpha_n) = F(\alpha_1)(\alpha_2)...(\alpha_n)$. Como $f(x)$ es un polinomio mínimo de α_n sobre $F(\alpha_1)(\alpha_2)...(\alpha_{n-1})$

$$[F(\alpha_1)(\alpha_2)...(\alpha_n) : F(\alpha_1)(\alpha_2)...(\alpha_{n-1})] \leq grado(f(x)) = n.$$

Como $(x-\alpha_1)(x-\alpha_2) \ldots (x-\alpha_{n-1})$ es un polinomio mínimo de α_{n-1} sobre $F(\alpha_1)(\alpha_2)...(\alpha_{n-2})$

$$[F(\alpha_1)(\alpha_2)...(\alpha_{n-1}) : F(\alpha_1)(\alpha_2)...(\alpha_{n-2})] \leq n-1.$$

Siguiendo este proceso obtenemos que

$$[F(\alpha_1, \alpha_2, ..., \alpha_n) : F] = [F(\alpha_1)...(\alpha_n) : F(\alpha_1)...(\alpha_{n-1})] \cdot [F(\alpha_1)...(\alpha_{n-1}) : F(\alpha_1)...(\alpha_{n-2})]$$
$$\cdot ... \cdot [F(\alpha_1) : F] \leq n(n-1)(n-2)..,1 = n! \ . \ \clubsuit$$

Ex. 207 *Sea E una extensión de F. Sea $\alpha \in E$ trascendente sobre F. Demostrar que los cuerpos $F(\alpha)$ y $F(x)$ son isomorfos.*

$\equiv$

Recordemos que un elemento α de una extensión E de F se dice que es trascendente sobre F siempre que no es algebraico, i.e., no existe polinomio alguno de $F[x]$ que tenga a α como raíz. Definimos

$$\varphi : F(x) \longrightarrow F(\alpha)$$

$$\frac{f(x)}{g(x)} \to \varphi(\frac{f(x)}{g(x)}) := \frac{f(\alpha)}{g(\alpha)} = f(\alpha) \cdot (g(\alpha))^{-1}.$$

φ bien definida: Como α no es algebraico sobre F, está claro que, $\forall \frac{f(x)}{g(x)} \in F(x)$, $g(\alpha) \neq 0$, entonces se puede calcular $f(\alpha) \cdot (g(\alpha))^{-1}$.
φ homomorfismo de cuerpos: Dadas $\frac{f(x)}{g(x)}, \frac{p(x)}{q(x)} \in F(x)$

$$\varphi(\frac{f(x)}{g(x)} + \frac{p(x)}{q(x)}) = \varphi(\frac{f(x)q(x)+p(x)g(x)}{g(x)q(x)}) = \frac{f(\alpha)q(\alpha)+p(\alpha)g(\alpha)}{g(\alpha)q(\alpha)} = \frac{f(\alpha)}{g(\alpha)} + \frac{p(\alpha)}{q(\alpha)} = \varphi(\frac{f(x)}{g(x)}) + \varphi(\frac{p(x)}{q(x)})$$

$$\varphi(\frac{f(x)}{g(x)}\frac{p(x)}{q(x)}) = \varphi(\frac{f(x)p(x)}{g(x)q(x)}) = \frac{f(\alpha)p(\alpha)}{g(\alpha)q(\alpha)} = \frac{f(\alpha)}{g(\alpha)}\frac{p(\alpha)}{q(\alpha)} = \varphi(\frac{f(x)}{g(x)})\varphi(\frac{p(x)}{q(x)}).$$

φ inyectiva: Si $\frac{f(x)}{g(x)} \in Ker(\varphi)$, entonces

$$0 = \varphi(\frac{f(x)}{g(x)}) = \frac{f(\alpha)}{g(\alpha)} \Rightarrow f(\alpha) = 0 \overset{(\alpha \ trasc.)}{\Rightarrow} f(x) = 0 \Rightarrow \frac{f(x)}{g(x)} = 0.$$

φ sobre: El conjunto imagen $\varphi(F(x))$ es un subcuerpo de $F(\alpha)$ que cumple

$$\left.\begin{array}{l} \forall c \in F \subset F[x] \subset F(x), \varphi(c) = c \to c \in \varphi(F(x)) \to F \subset \varphi(F(x)) \\ \varphi(x) = \alpha \to \alpha \in \varphi(F(x)) \end{array}\right\}$$

$$\Rightarrow F(\alpha) \subset \varphi(F(x)) \subset F(\alpha).$$

Por tanto, $\varphi(F(x)) = F(\alpha)$. $\clubsuit$

Ex. 208 *Demostrar que dos cuerpos finitos con el mismo número de elementos son isomorfos.*

≡

Los razonamientos que vamos a emplear pueden verse en [6, p. 218].

Lema 6 *Dado un cuerpo finito F de cardinal q, existen un número primo p y un subcuerpo F' de F tales que $q = p^n$, con $n = [F : F']$.*

≡

Considerando la aplicación

$$\begin{array}{rccl} \varphi & : & \mathbf{Z} & \longrightarrow & F \\ & & k & \to & \varphi(k) := 1 + 1 + \overset{(n)}{\ldots} + 1 = k \cdot 1, \end{array}$$

está claro que φ es un homomorfismo de anillos (i.e., conserva la suma y el producto) y $Ker(\varphi)$ es un ideal de $\mathbf{Z}$. Como $\mathbf{Z}$ es un anillo principal, tenemos que existe un primo p tal que $Ker(\varphi) = (\ p\ )$, donde $(\ p\ )$ representa al ideal de $\mathbf{Z}$ generado por p (todos los múltiplos de p). Aplicando el teorema del isomorfismo

$$\mathbf{Z}_p \ = \ \mathbf{Z}/(\ p\ ) \ = \ \mathbf{Z}/Ker(\varphi) \ \cong \ \varphi(\mathbf{Z}) \ =: F' \ \subset \ F\ .$$

Consecuentemente, F' es un subcuerpo de F que es isomorfo a $\mathbf{Z}/(\ p\ )$. Al ser F finito, $[F : F']$ es finito. Sea $n := [F : F']$. Entonces, F es un espacio vectorial de dimensión n sobre F' y

$$q \ = \ card(F) \ = \ card(F')^n \ = \ card(\mathbf{Z}_p)^n \ = \ p^n\ . \bullet$$

Lema 7 *Dado un cuerpo finito F de cardinal q, sea F' el subcuerpo de F isomorfo a Z_p tal que $q = p^n$, con $n = [F : F']$. Entonces, si $f(x) = x^q - x \in F'[x]$, se tiene que F es un cuerpo de descomposición de $f(x)$.*

≡

Como F^* es un grupo multiplicativo cíclico de oreden $q - 1$, queda claro que todo elemento de F es raíz de $f(x)$. Por tanto, si $F = \{0, a_1, a_2, ..., a_{q-1}\}$, tenemos que

$$f(x) \ = \ x^q \ - \ x \ = \ x(x - a_1)(x - a_2)...(x - a_{q-1}).$$

Ello prueba que F es un cuerpo raíz de $f(x)$. $\bullet$

Lema 8 *Sean E y E' dos extensiones del cuerpo F en donde se descompone el polinomio $f(x) \in F[x]$. Demostrar que existe un isomorfismo φ del cuerpo raíz de $f(x)$ en E en el cuerpo raíz de $f(x)$ en E' tal que, $\forall c \in F$, $\varphi(c) = c$.*

≡

Suponiendo que $grado(f(x)) = m$, podemos escribir

$$\begin{array}{l} f(x) \ = \ a(x - \alpha_1)(x - \alpha_2)...(x - \alpha_m) \\ f(x) \ = \ a(x - \alpha'_1)(x - \alpha'_2)...(x - \alpha'_m) \\ a \in F, \ \ \alpha_1, \alpha_2, ..., \alpha_m \in E, \ \ \alpha'_1, \alpha'_2, ..., \alpha'_m \in E'. \end{array}$$

Si representamos como $F_E(\alpha_1, ..., \alpha_m)$ y $F_{E'}(\alpha'_1, ..., \alpha'_m)$ a los cuerpos raíz de $f(x)$ en E y en E', respectivamente, podemos definir

$$\begin{array}{rcl} \varphi & : & F_E(\alpha_1, ..., \alpha_m) \longrightarrow F_{E'}(\alpha'_1, ..., \alpha'_m) \\ & & \sum c\, \alpha_1^{i_1} ... \alpha_m^{i_m} \rightarrow \varphi(\sum c\, \alpha_1^{i_1} ... \alpha_m^{i_m}) := \sum c\, \alpha'_1{}^{i_1} ... \alpha'_m{}^{i_m}. \end{array}$$

Es fácil ver que φ está bien definida, que se trata de un homomorfismo de cuerpos y que $\varphi(c) = c$, $\forall c \in F$. Además, φ es inyectiva y, como $\varphi[F_E(\alpha_1, ..., \alpha_m)]$ y $F_{E'}(\alpha'_1, ..., \alpha'_m)$ son cuerpos raíz de un mismo polinomio en un mismo cuerpo, se tiene que

$$card[F_E(\alpha_1, ..., \alpha_m)] = card[\varphi(F_E(\alpha_1, ..., \alpha_m)] = card[F_{E'}(\alpha'_1, ..., \alpha'_m)],$$

es decir, φ es biyectiva. •

Volviendo al enunciado de nuestro ejercicio, Sean F y E dos cuerpos finitos del mismo cardinal q. Del primero de los tres lemas anteriores, existe un primo p tal que $\mathbf{Z}_p$ es isomorfo a un subcuerpo de F y a uno de E. Considerando $\mathbf{Z}_p$ como subcuerpo de F y de E, del segundo lema se tiene que F y E son extensiones de $\mathbf{Z}_p$ en las que se descompone el polinomio $x^q - x \in \mathbf{Z}_p[x]$. Del tercero de los lemas vistos, podemos afirmar que F y E son isomorfos. ♣

Ex. 209 *Sea E una extensión de F. Sea $\alpha \in E$ trascendente sobre F. Hallar el grado de $F(\alpha)$ sobre $F(\frac{\alpha^4}{4\alpha^3-1})$.*

≡

Al ser $\alpha \in E$ trascendente sobre F, sabemos que

$$F(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} \ : \ f(x), g(x) \in F[x],\ g(x) \neq 0\}.$$

Por tanto, $\lambda := \frac{\alpha^4}{4\alpha^3-1} \in F(\alpha)$. Consecuentemente, $F(\lambda) \subset F(\alpha)$. Además, α es algebraico sobre $F(\lambda)$ pues

$$\alpha^4 - 4\lambda\alpha^3 + \lambda = 0 \Rightarrow \left\{ \begin{array}{l} f(x) := x^4 - 4\lambda x^3 + \lambda \in F(\lambda)[x] \\ f(\alpha) = 0. \end{array} \right.$$

Distinguimos dos casos:
Uno. $\alpha \in F(\lambda)$. Entonces $F(\lambda) = F(\alpha)$ y $[F(\alpha) : F(\lambda)] = 1$.
Dos. $\alpha \notin F(\lambda)$. Ahora tenemos que $\frac{\alpha^3}{4\alpha^3-1} \notin F(\lambda)$, de lo contrario

$$\alpha = \lambda \cdot (\frac{\alpha^3}{4\alpha^3 - 1})^{-1} \in F(\lambda).$$

Observemos que $f(x)$ se puede factorizar del siguiente modo

$$f(x) = (x - \alpha) \cdot (x^3 - \frac{\alpha}{4\alpha^3 - 1} x^2 - \frac{\alpha^2}{4\alpha^3 - 1} x - \frac{\alpha^3}{4\alpha^3 - 1}).$$

Entonces

$$\left.\begin{array}{l} x-\alpha \notin F(\lambda)[x] \\ x^3-\frac{\alpha}{4\alpha^3-1}x^2-\frac{\alpha^2}{4\alpha^3-1}x-\frac{\alpha^3}{4\alpha^3-1} \notin F(\lambda)[x] \end{array}\right\} \Rightarrow f(x) \text{ irred. sobre } F(\lambda).$$

Por tanto, $f(x)$ es un polinomio mínimo de α sobre $F(\lambda)$, de donde $[F(\alpha) : F(\lambda)] = grado(f(x)) = 4$. ♣

Ex. 210 *Sea A el conjunto de los números algebraicos en $\mathbf{C}$.*

a) Demostrar que A es un subcuerpo de $\mathbf{C}$.

b) Demostrar que A es numerable (por tanto, existen números trascendentes).

≡

a) Sean $a, b \in A$. De un ejercicio anterior, sabemos que $\mathbf{Q}(a,b) = \mathbf{Q}(a)(b)$. Entonces, como $\mathbf{Q}(a)$ es una extensión algebraica de $\mathbf{Q}$ y $\mathbf{Q}(a)(b)$ es una extensión algebraica de $\mathbf{Q}(a)$, tenemos que $\mathbf{Q}(a,b)$ es una extensión algebraica de $\mathbf{Q}$. Es decir, $\mathbf{Q}(a,b) \subset A$. Evidentemente

$$\left.\begin{array}{l} a-b \in \mathbf{Q}(a,b) \rightarrow a-b \in A \\ a \cdot b \in \mathbf{Q}(a,b) \rightarrow a \cdot b \in A. \end{array}\right\} \Rightarrow A \text{ es subcuerpo de } \mathbf{C}.$$

b) Dado $f(x) \in \mathbf{Q}[x]$, representamos por $A(f(x))$ al conjunto de las raíces de $f(x)$ en $\mathbf{C}$. Claramente, $A(f(x)) \subset A$. Además, por definición de número algebraico se tiene que

$$A = \bigcup_{f(x)\in\mathbf{Q}[x]} A(f(x)).$$

Para cada $f(x) \in \mathbf{Q}[x]$, $A(f(x))$ es un conjunto finito (numerable, por tanto). Puesto que toda unión numerable de conjuntos numerables es numerable, todo se reduce a ver que $\mathbf{Q}[x]$ es numerable. Definiendo, para cada $n \in \mathbf{N} \cup \{0\} \cup \{-\infty\}$, $\mathbf{Q}_n[x]$ como el conjunto de todos los polinomios de $\mathbf{Q}[x]$ de grado n, está claro (ya que $\mathbf{Q}$ es numerable) que $\mathbf{Q}_n[x]$, equipotente con $\mathbf{Q}^{n+1}$, es numerable. De ahí que podamos afirmar que

$$\mathbf{Q}[x] = \bigcup_{n\in\mathbf{N}\cup\{0\}\cup\{-\infty\}} \mathbf{Q}_n[x] \qquad \text{es numerable. } ♣$$

Ex. 211 *Demostrar que, si $\alpha, \beta \in \mathbf{C}$ son trascendentes, entonces o bien $\alpha+\beta$, o bien $\alpha \cdot \beta$, es trascendente.*

≡

Supongamos, razonando por refutación, que ambos números $\alpha+\beta$ y $\alpha\beta$ son algebraicos. Consideremos el polinomio

$$\left.\begin{array}{l} f(x) := x^2-(\alpha+\beta)x+\alpha\beta \in \mathbf{Q}(\alpha+\beta,\alpha\beta)[x] \\ f(\alpha) = 0 = f(\beta) \end{array}\right\}$$

$$\Rightarrow \alpha, \beta \text{ son algebraicos sobre } \mathbf{Q}(\alpha+\beta,\alpha\beta).$$

Entonces $\mathbf{Q}(\alpha+\beta,\alpha\beta,\alpha,\beta)$ es una extensión algebraica de $\mathbf{Q}(\alpha+\beta,\alpha\beta)$, que a su vez, al ser $\alpha+\beta$ y $\alpha\beta$ algebraicos, es una extensión algebraica de $\mathbf{Q}$. Por transitividad, $\mathbf{Q}(\alpha+\beta,\alpha\beta,\alpha,\beta)$ es una extensión algebraica de $\mathbf{Q}$, lo que implica que α y β son algebraicos, una contradicción. ♣

Ex. 212 *Un polinomio $f(x) \in F[x]$ se dice que es separable siempre que $mcd(f(x), f'(x))$ es constante, i.e., $f(x)$ y $f'(x)$ son primos entre sí, siendo $f'(x)$ el polinomio derivada. Sea E una extensión de F en donde $f(x)$ se descompone. Demostrar que $f(x)$ es separable si y sólo si las raíces de $f(x)$ en E son distintas (de ahí el calificativo de "separable").*

$\equiv$

$[\Rightarrow]$ Aplicando el lema de Bezout, si $f(x)$ es separable, existen $p(x), q(x) \in F[x]$ tales que $1 = p(x)f(x) + q(x)f'(x)$. Razonando por refutación, supongamos que $f(x)$ admite una raíz múltiple $\alpha \in E$. Entonces existe $g(x) \in F[x]$ para el cual

$$\left.\begin{array}{l} f(x) = (x-\alpha)^2 \cdot g(x) \\ f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) = (x-\alpha)[2g(x) + (x-\alpha)g'(x)]. \end{array}\right\}$$

$$\Rightarrow 1 = p(\alpha)f(\alpha) + q(\alpha)f'(\alpha) = 0. \text{ Absurdo}$$

$[\Leftarrow]$ Suponiendo que todas las raíces de $f(x)$ en E son distintas, como E es un cuerpo raíz de $f(x)$, podemos escribir, si $grado(f(x)) = n$,

$$f(x) = c\,(x-\alpha_1)(x-\alpha_2)\,...\,(x-\alpha_n), \quad c \in F, \quad \alpha_1, \alpha_2, .., \alpha_n \in E.$$

Entonces

$$f'(x) = c \sum_{i=1}^{n} \prod_{1 \le j \ne i \le n} (x-\alpha_j).$$

Claramente, para $i = 1, 2, ..., n$, $x - \alpha_i$ no divide a $f'(x)$, ya que divide a todos los sumandos de $f'(x)$ excepto a uno: $(x-\alpha_1)...(x-\alpha_{i-1})(x-\alpha_{i+1})...(x-\alpha_n)$, al ser las raíces distintas. Por tanto, ningún factor de $f(x)$ es factor de $f'(x)$, es decir, $f(x)$ y $f'(x)$ son primos entre sí. ♣

Ex. 213

a) Demostrar que un polinomio irreducible es separable si y sólo si su derivada es distinta de cero.

b) Demostrar también que todo polinomio irreducible sobre un cuerpo de característica cero es separable.

$\equiv$

a)

$[\Rightarrow]$ Sea $f(x) \in F[x]$ irreducible y separable. Entonces, $grado(f(x)) \ge 1$ y existen $p(x), q(x) \in F[x]$ tales que $1 = p(x)f(x) + q(x)f'(x)$. Si $f'(x) = 0$, se tendría que $1 = p(x)q(x)$, lo que contradice que $f(x)$ tiene grado positivo.

$[\Leftarrow]$ Sea $f(x) \in F[x]$ irreducible tal que $f'(x) \ne 0$. Al ser $f(x)$ irreducible no tiene divisores propios (de grado positivo), por lo tanto $f(x)$ y $f'(x)$ son primos entre sí, es decir, $f(x)$ es separable.

b) Sea $f(x) \in F[x]$ irreducible, con $carac(F) = 0$. Aplicando el apartado a), todo se reduce a ver que $f'(x) \ne 0$. Supongamos que $f(x) = c_0 + c_1 x + ... + c_n x^n$, $c_n \ne 0$, y que $f'(x) = 0$. Entonces, derivando $n-1$ veces

$$0 = f^{(n)}(x) = n! \cdot c_n \overset{(carac(F)=0)}{\Rightarrow} c_n = 0. \text{ Absurdo. } ♣$$

Ex. 214 *Un cuerpo F de característica p se dice que es perfecto siempre que*

$$\forall a \in F, \quad x^p - a \text{ tiene alguna raiz en } F.$$

Demostrar que todo cuerpo finito es perfecto.

≡

Antes de ponernos a resolver el ejercicio, indiquemos que, por convenio, todo cuerpo de característica cero es perfecto.

Sea F un cuerpo finito. Si $carac(F) = p$, se vió en un problema anterior que el cuerpo $\mathbf{Z}_p$ está inmerso (es isomorfo a un subcuerpo) en F, de manera que, si $[F : \mathbf{Z}_p] = n$, entonces $card(F) = p^n$. Así, como F^* es un grupo multiplicativo cíclico de orden $p^n - 1$, dado un elemento $a \in F$, suponemos que $a \neq 0$ (si no, $x^p - a = x^p$ tiene raíz en $x = 0$),

$$1 = a^{p^n-1} \Rightarrow a^{p^n} = a \rightarrow (a^{p^n-1})^p - a = 0,$$

es decir, a^{p^n-1} es una raíz del polinomio $x^p - a$. ♣

Ex. 215 *Sea F un cuerpo perfecto de característica distinta de cero. Demostrar que todo polinomio irreducble sobre F es separable en F.*

≡

Para resolver el ejercicio usamos un ejercicio anterior. Así, si $f(x) = c_0 + c_1 + ... + c_n x^n \in F[x]$ es irreducible sobre F, vamos a ver que $f'(x) \neq 0$. De lo contrario

$$0 = f'(x) = c_1 + 2c_2 x + ... + nc_n x^{n-1} \Rightarrow i \cdot c_i = 0,\ 1 \leq i \leq n \Rightarrow \forall i = 1, 2, ..., n \begin{cases} c_i = 0 \\ ó \\ p \mid i \end{cases}$$

De donde, para cierto $m \in \mathbf{N}$,

$$f(x) = c_0 + c_p x^p + c_{2p} x^{2p} + ... + c_{mp} x^{mp}.$$

Como F es un cuerpo perfecto, para cada $i = 0, 1, ..., m$, existe $a_i \in F$ tal que $c_{ip} = a_i^p$. Así

$$f(x) = a_0^p + a_1^p x^p + a_2^p x^{2p} + ... + a_m^p x^{mp} = (a_0 + a_1 x + a_2 x^2 + ... + a_m x^m)^p,$$

donde esta última igualdad se debe a que $carac(F) = p$ (puede demostrarse inductivamente sin mucha dificultad). Hemos obtenido pues que $f(x)$ es reducible sobre F, lo que es una contradicción. ♣

Ex. 216 *Sea E una extensión de F. Un elemento $\alpha \in E$ se dice que es separable sobre F siempre que existe un polinomio $f(x) \in F[x]$ separable tal que $f(\alpha) = 0$.*

a) Demostrar que, si $\alpha \in E$ es separable, entonces todo polinomio mínimo de α sobre F es separable.

b) Una extensión E de F se dice que es separable cuando todo elemento de E es separable sobre F. Demostrar que toda extensión algebraica de un cuerpo perfecto es separable.

$\equiv$

a) Sea $\alpha \in E$ separable sobre F. Por definición, existe $f(x) \in F[x]$ separable sobre F tal que $f(\alpha) = 0$. Como α es algebraico sobre F, sea $g(x)$ un polinomio mínimo de α sobre F. Sabemos que entonces $g(x)$ es un divisor de $f(x)$. Sea

$$f(x) \;=\; c \cdot (x-\alpha)(x-\lambda_1)...(x-\lambda_n), \quad c \in F,$$

la factorización de $f(x)$ en su cuerpo raíz K. Como $f(x)$ es separable, de un problema anterior, sabemos que todas sus raíces son distintas. Obviamente, como $g(x) \mid f(x)$, la factorización de $g(x)$ es

$$g(x) \;=\; d \cdot (x-\alpha)(x-\lambda_{i_1})...(x-\lambda_{i_m}), \quad d \in F, \quad i_1, i_2, ..., i_m \in \{1, 2, ..., n\}.$$

Al descomponerse en raíces distintas deducimos que $g(x)$ es separable.

b) Sea E una extensión algebraica de F, siendo F un cuerpo perfecto. Dado $\alpha \in E$, sea $f(x)$ un polinomio mínimo de α sobre F. De un problema resuelto antes, sabemos que un polinomio irreducible sobre un cuerpo perfecto es separable. Por tanto, $f(x)$ es separable, lo que implica que α es un elemento separable y E es una extensión separable. ♣

Ex. 217 *Demostrar que todo cuerpo imperfecto admite una extensión algebraica inseparable.*

$\equiv$

Sea F un cuerpo imperfecto. Obligatoriamente, la característica de F ha de ser positiva, sea $carac(F) = p$. Así, existe $a \in F$ de modo que $x^p - a$ no tiene raíces en F. Sea $E := F(\alpha)$, donde α es una raíz del polinomio $x^p - a$. Claramente E es una extensión algebraica de F. Veamos que no es separable. De serlo, α sería separable sobre F. Del ejercicio anterior, si $f(x) \in F[x]$ es un polinomio mínimo de α sobre F, tenemos que $f(x)$ es separable. Además, $f(x) \mid x^p - a$, por lo que existe $g_1(x) \in F[x]$ tal que $x^p - a = f(x)g_1(x)$. Derivando

$$0 \;=\; px^{p-1} \;=\; f'(x)g_1(x) \;+\; f(x)g_1'(x) \;\overset{(f(x)\ separable)}{\Rightarrow}\; f(x) \mid g_1(x).$$

Así, existe $g_2(x) \in F[x]$ tal que $g_1(x) = f(x)g_2(x)$. Entonces

$$x^p - a \;=\; (f(x))^2 g_2(x).$$

Volviendo a derivar obtenemos que $f(x) \mid g_2(x)$. Repitiendo este proceso unas cuantas veces (lo que marque el grado de $f(x)$) se llega a que $f(x)$ es divisor de un polinomio de menos grado, lo que es absurdo. ♣

Ex. 218 *Si F es un cuerpo perfecto, demostrar que toda extensión algebraica de F es perfecta.*

$\equiv$

De ejercicios anteriores sabemos que un cuerpo es perfecto si y sólo si toda extensión algebraica es separable. Por tanto, si E es una extensión algebraica de F, todo consiste

en ver que, si E' es una extensión algebraica de E, entonces E' es separable. Al ser E' algebraica sobre E y E algebraica sobre F, tenemos que E' es una extensión algebraica sobre F. Como, por hipótesis, F es perfecto, se tiene que E' es una extensión separable sobre F. Claramente, E' es una extensión separable sobre E. Por tanto, E es un cuerpo perfecto. ♣

Ex. 219 *Dado $\alpha \in E$, donde E es una extensión del cuerpo perfecto F, con $carac(F) = p$, demostrar que α es un elemento separable si y sólo si $F(\alpha^p) = F(\alpha)$.*

≡

[$\Rightarrow$] Como $\alpha^p \in F(\alpha)$, se tiene que $F(\alpha^p) \subset F(\alpha)$. Al suponer que $\alpha \in E$ separable sobre F, por definición, existe un polinomio separable $f(x) \in F[x]$ tal que $f(\alpha) = 0$. De un ejercicio anterior sabemos que no supone pérdida de generalidad asumir que $f(x)$ es un polinomio mínimo de α sobre F. Entonces $[F(\alpha) : F] = grado(f(x))$. Sea $f(x) = c_0 + c_1 x + ... + c_n x^n$. Consideremos el polinomio

$$g(x) := c_0^p + c_1^p x + ... + c_n^p x^n \in F[x].$$

Como

$$g(\alpha^p) = c_0^p + c_1^p \alpha^p + ... + c_n^p (\alpha^p)^n = (c_0 + c_1 \alpha + ... + c_n \alpha^n)^p = f(\alpha)^p = 0,$$

tenemos que $g(x)$ es un polinomio mínimo de α^p sobre F. Por tanto

$$\left.\begin{array}{l} [F(\alpha^p) : F] = n = [F(\alpha) : F] \\ F(\alpha^p) \subset F(\alpha) \end{array}\right\} \overset{(F(\alpha^p) \text{ subesp.vect. de } F(\alpha))}{\Rightarrow} F(\alpha^p) = F(\alpha).$$

[$\Leftarrow$] Supongamos que $F(\alpha^p) = F(\alpha)$. Entonces, como $\alpha \in F(\alpha^p)$, existe un polinomio $f(x) \in F[x]$ tal que $\alpha = f(\alpha^p)$. Así, α es raíz del polinomio $x - f(x^p) \in F[x]$, por lo que $F(\alpha)$ es una extensión algebraica del cuerpo perfecto F. De un ejercicio anterior sabemos que $F(\alpha)$ es una extensión separable, de donde α es separable sobre F. ♣

Ex. 220 *Sea E una extensión finita del cuerpo perfecto F, con $carac(F) = p$. Sea $E^{(p)}$ el menor subcuerpo de E que contiene a $F \cup \{\alpha^p : \alpha \in E\}$. Demostrar que E es una extensión separable de F si y sólo si $E^{(p)} = E$.*

≡

[$\Rightarrow$] Supongamos que E es una extensión separable de F. Del ejercicio previo, dado $\alpha \in E$, $F(\alpha^p) = F(\alpha)$. Es decir

$$\forall \alpha \in E, \quad \alpha \in F(\alpha) = F(\alpha^p) \subset E^{(p)} \Rightarrow E = E^{(p)}.$$

[$\Leftarrow$] Supongamos que $E = E^{(p)}$. Entonce $\begin{array}{l} \varphi : E \to E \\ \alpha \to \varphi(\alpha) := \alpha^p \end{array}$ es un isomorfismo de cuerpos, de hecho esta aplicación, dado que $carac(F) = p$, es siempre un homomorfismo inyectivo, bajo la hipótesis actual, y F perfecto, se tiene que también es sobre. Así

$$\forall \alpha \in E, \quad [F(\alpha) : F] = [F(\alpha^p) : F] \overset{(F(\alpha^p) \text{ subesp.vect. de } F(\alpha))}{\Rightarrow} F(\alpha^p) = F(\alpha).$$

Del ejercicio anterior podemos afirmar que α es separable sobre F, lo que demuestra que E es una extensión separable de F. ♣

Ex. 221 *[Teorema del elemento primitivo]*
Demostrar que toda extensión separable finita de un cuerpo es una extensión simple.

≡

Una extensión algebraica E del cuerpo F se dice que es simple siempre que existe $\alpha \in E$ tal que $E = F(\alpha)$, en dicho caso, a α se le denomina elemento primitivo. Distinguimos dos casos

Uno. F es finito. Entonces, como E es extensión finita de F, tenemos que E es un cuerpo finito. Sabemos que E^* es un grupo cíclico multiplicativo, por lo que, si $E^* = \langle\ \alpha\ \rangle$, es evidente que $E = F(\alpha)$.

Dos. F es infinito. E se puede escribir de la forma

$$E \ = \ F(\beta_1, \beta_2, ..., \beta_k)\ .$$

Utilizando un razonamiento inductivo, todo se reduce a verlo para $k = 2$, es decir, para $E = F(\beta_1, \beta_2)$. Entonces, ya que E es separable, sean $f_1(x), f_2(x)$ polinomios mínimos separables de β_1 y β_2 sobre F, respectivamente. Por tanto, ambos polinomios se descomponen en sus respectivos cuerpos raíz, i.e., admiten raíces distintas que podemos tomar como

$$\begin{array}{l} \beta_1 = \alpha_1, \alpha_2, ..., \alpha_n \ \text{ raices de } f_1(x) \\ \beta_2 = \gamma_1, \gamma_2, ..., \gamma_m \ \text{ raices de } f_2(x). \end{array}$$

Como F es infinito, podemos encontrar un elemento

$$c \ \in \ F \setminus \{\frac{\alpha_i - \alpha_1}{\gamma_1 - \gamma_j} \ : \ 2 \leq i \leq n, \ \ 2 \leq j \leq m\}, \ \ c \neq 0.$$

Sea $\delta := \beta_1 + c\beta_2$. Entonces, como $\delta \in F(\beta_1, \beta_2)$, tenemos que $F(\delta) \subset F(\beta_1, \beta_2) = E$. Consideramos el polinomio $h(x) := f_1(\delta - cx) \in F(\delta)[x]$. Así

$$h(\beta_2) \ = \ f_1(\delta - c\beta_2) \ = \ f_1(\beta_1) \ = \ 0,$$

implica que, si $g(x)$ es un polinomio mínimo de β_2 sobre $F(\delta)$, se tiene que $g(x) \mid h(x)$ y $g(x) \mid f_2(x)$. Pero $h(x)$ y $f_2(x)$ no poseen más raíz en común que β_2, ya que, para $j = 2, 3, ..., m$

$$h(\gamma_j) \ = \ f_1(\delta - c\gamma_j) \ = \ f_1(\alpha_1 + c(\gamma_1 - \gamma_j)) \ \overset{(defin.\ c)}{\neq} \ 0.$$

Por tanto, $g(x) = a(x - \beta_2)$, $a \in F(\delta)$. Entonces

$$\left.\begin{array}{l} \beta_2 \in F(\delta) \\ \beta_1 = \delta - c\beta_2 \in F(\delta) \end{array}\right\} \ \Rightarrow \ F(\beta_1, \beta_2) \ \subset \ F(\delta). \ \clubsuit$$

Ex. 222 *Hallar un elemento primitivo sobre* $\mathbf{Q}$ *para cada uno de los cuerpos:* $\mathbf{Q}(\sqrt{2}, \sqrt{3})$, $\mathbf{Q}(\mathbf{i}, \sqrt{2})$, $\mathbf{Q}(\sqrt{3}, 2e^{\frac{2\pi \mathbf{i}}{3}})$.

$\equiv$

Para $\mathbf{Q}(\sqrt{2},\sqrt{3})$. Veamos que $\mathbf{Q}(\sqrt{2},\sqrt{3}) = \mathbf{Q}(\sqrt{2}+\sqrt{3})$:

$[\supset]$ Evidente.

$[\subset]$

$$\left.\begin{array}{l}(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6} \to \sqrt{6} \in \mathbf{Q}(\sqrt{2}+\sqrt{3}) \\ \sqrt{6}(\sqrt{2}+\sqrt{3}) = 2\sqrt{3}+3\sqrt{2} \in \mathbf{Q}(\sqrt{2}+\sqrt{3})\end{array}\right\} \Rightarrow \sqrt{2} = (2\sqrt{3}+3\sqrt{2}) - 2(\sqrt{2}+\sqrt{3}).$$

Por tanto $\sqrt{2} \in \mathbf{Q}(\sqrt{2}+\sqrt{3})$. Finalmente

$$\left.\begin{array}{l}\sqrt{6} \in \mathbf{Q}(\sqrt{2}+\sqrt{3}) \\ \sqrt{2} \in \mathbf{Q}(\sqrt{2}+\sqrt{3})\end{array}\right\} \Rightarrow \sqrt{3} = \frac{\sqrt{6}}{\sqrt{2}} \in \mathbf{Q}(\sqrt{2}+\sqrt{3}).$$

Para $\mathbf{Q}(\mathbf{i},\sqrt{2})$. Veamos que $\mathbf{Q}(\mathbf{i},\sqrt{2}) = \mathbf{Q}(\sqrt{2}+\mathbf{i})$:

$[\supset]$ Evidente.

$[\subset]$

$$\frac{1}{\sqrt{2}+\mathbf{i}} = \frac{\sqrt{2}-\mathbf{i}}{3} \to \sqrt{2}-\mathbf{i} \in \mathbf{Q}(\sqrt{2}+\mathbf{i}).$$

Finalmente

$$\left.\begin{array}{l}\sqrt{2}-\mathbf{i} \in \mathbf{Q}(\sqrt{2}+\mathbf{i}) \\ \sqrt{2}+\mathbf{i} \in \mathbf{Q}(\sqrt{2}+\mathbf{i})\end{array}\right\} \Rightarrow \left\{\begin{array}{l}\sqrt{2} \in \mathbf{Q}(\sqrt{2}+\mathbf{i}) \\ \mathbf{i} \in \mathbf{Q}(\sqrt{2}+\mathbf{i}).\end{array}\right.$$

Para $\mathbf{Q}(\sqrt{3},2\mathrm{e}^{\frac{2\pi\mathbf{i}}{3}})$. Veamos que $\mathbf{Q}(\sqrt{3},2\mathrm{e}^{\frac{2\pi\mathbf{i}}{3}}) = \mathbf{Q}(\sqrt{3}(1+\mathbf{i}))$:

$[\supset]$ Evidente, ya que

$$\left.\begin{array}{rcl}2\mathrm{e}^{\frac{2\pi\mathbf{i}}{3}} & = & 2(\cos\frac{2\pi}{3}+\mathbf{i}\sin\frac{2\pi}{3}) = -1+\mathbf{i}\sqrt{3} \\ 2\mathrm{e}^{\frac{-2\pi\mathbf{i}}{3}} & = & 2(\cos\frac{-2\pi}{3}+\mathbf{i}\sin\frac{-2\pi}{3}) = -1-\mathbf{i}\sqrt{3}\end{array}\right\} \Rightarrow \mathbf{i}\sqrt{3} \in \mathbf{Q}(2\mathrm{e}^{\frac{2\pi\mathbf{i}}{3}}) \subset \mathbf{Q}(\sqrt{3},2\mathrm{e}^{\frac{2\pi\mathbf{i}}{3}}).$$

$[\subset]$

$$(\sqrt{3}(1+\mathbf{i}))^2 = 6\mathbf{i} \to \mathbf{i} \in \mathbf{Q}(\sqrt{3}(1+\mathbf{i})) \to 1+\mathbf{i} \in \mathbf{Q}(\sqrt{3}(1+\mathbf{i}))$$

$$\to \sqrt{3} = \frac{\sqrt{3}(1+\mathbf{i})}{1+\mathbf{i}} \in \mathbf{Q}(\sqrt{3}(1+\mathbf{i})).$$

Además, de lo visto antes

$$2\mathrm{e}^{\frac{2\pi\mathbf{i}}{3}} = -1+\mathbf{i}\sqrt{3} \in \mathbf{Q}(\sqrt{3}(1+\mathbf{i})). \clubsuit$$

Capítulo 3

Teoría de Galois

3.1. El grupo de automorfismos de un cuerpo

Ex. 223 *En general, dado un cuerpo F, representamos por $\mathcal{G}(F)$ al grupo de todos los automorfismos de F, i.e., homomorfismos de cuerpos (hay quien dice de anillos) biyectivos, con la operación de composición. Demostrar que $\mathcal{G}(\mathbf{Q})$ y $\mathcal{G}(\mathbf{Z}_p)$ son grupos triviales.*

≡

Veamos que $\mathcal{G}(\mathbf{Q}) = \{1_{\mathbf{Q}}\}$, donde $1_{\mathbf{Q}}$ indica la identidad de $\mathbf{Q}$. Dado $f \in \mathcal{G}(\mathbf{Q})$, tenemos

$$\left.\begin{array}{l} f(0)=0 \\ f(1)=1 \\ f(-1)=-1 \end{array}\right\} \Rightarrow \forall n \in \mathbf{N} \left\{\begin{array}{l} f(n) = f(1+1+\overset{(n)}{\ldots}+1) = f(1)+f(1)+\overset{(n)}{\ldots}+f(1) = n \\ f(-n) = f(-1-1-\overset{(n)}{\ldots}-1) = -n \end{array}\right\}$$

$$\Rightarrow \ f_{|\mathbf{Z}} = 1_{\mathbf{Z}}.$$

Finalmente, si $\frac{m}{n} \in \mathbf{Q}$

$$f(\frac{m}{n}) \cdot n \overset{(n\in\mathbf{Z})}{=} f(\frac{m}{n}) f(n) \ = \ f(\frac{m}{n} \cdot n) \ = \ f(m) \overset{(m\in\mathbf{Z})}{=} m \ \Rightarrow \ f(\frac{m}{n}) \ = \ \frac{m}{n}.$$

Veamos que $\mathcal{G}(\mathbf{Z}_p) = \{1_{\mathbf{Z}_p}\}$. Si $f \in \mathcal{G}(\mathbf{Z}_p)$, entonces (escribimos $\{0,1,2,...,p-1\}$ para $\mathbf{Z}_p$)

$$\left.\begin{array}{l} f(0)=0 \\ f(1)=1 \end{array}\right\} \Rightarrow \forall n \in \mathbf{Z}_p, \quad f(n) = f(1+1+\overset{(n)}{\ldots}+1) = f(1)+f(1)+\overset{(n)}{\ldots}+f(1) = n. \ \clubsuit$$

Ex. 224 *Determinar el grupo de automorfismos de un cuerpo de 4 elementos.*

≡

Sea F un cuerpo tal que $card(F) = 4$. De la teoría de cuerpos, sabemos que $carac(F)$ es un número primo divisor de su cardinal y mayor que 1, por tanto, $carac(F) = 2$ (notar

que $card(F) = 2^2$). Admás, puesto que F^* es un grupo multiplicativo cíclico, podemos escribir

$$F = \{ 0,\ 1,\ a,\ a^2 \}.$$

Con todo este preparativo, veamos que $\mathcal{G}(F) = \{1_F, f\}$, donde

$$\begin{array}{rccl} f & : & F & \longrightarrow & F \\ & & 0 & \to & 0 \\ & & 1 & \to & 1 \\ & & a & \to & a^2 \\ & & a^2 & \to & a. \end{array}$$

Primero comprobempos que f es en efecto un automorfismo: Biyectivo lo es.

$$\left.\begin{array}{l} f(1+a) \overset{(1+a=a^2)}{=} a = 1 + a^2 = f(1) + f(a) \\ f(1+a^2) \overset{(1+a^2=a)}{=} a^2 = 1 + a = f(1) + f(a^2) \\ f(a+a^2) \overset{(a+a^2=a(1+a)=a^3=1)}{=} 1 = a^2 + a = f(a) + f(a^2) \\ f(a \cdot a^2) = f(1) = 1 = a^2 \cdot a = f(a) \cdot f(a^2 \end{array}\right\} \Rightarrow f \text{ es automorfismo.}$$

Por tanto, todo consiste en ver que, si $g \in \mathcal{G}(F)$ es tal que $g \neq 1_F$, entonces $g = f$. Para ello

$$\left.\begin{array}{l} g(0) = 0 \\ g(1) = 1 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} g(a) \notin \{0, 1, a\} \\ g(a) = a^2 \\ g(a^2) = g(a)^2 = a^4 = a^3 \cdot a = a \end{array}\right\} \Rightarrow g = f. \clubsuit$$

Nota 22 Hemos demostrado por tanto que, si F es un cuerpo de 4 elementos, entonces su grupo de automorfismos es $\mathbf{Z}_2$.

Ex. 225 *Determinar el grupo de automorfismos de* $\mathbf{Q}(\mathbf{i})$ *y de* $\mathbf{Q}(\sqrt{2})$.

$\equiv$

Veamos primero que $\mathcal{G}(\mathbf{Q}(\mathbf{i})) = \{1_{\mathbf{Q}(\mathbf{i})}, \varphi\}$, siendo

$$\begin{array}{rccl} \varphi & : & \mathbf{Q}(\mathbf{i}) & \longrightarrow & \mathbf{Q}(\mathbf{i}) \\ & & a + b\mathbf{i} & \to & a - b\mathbf{i}. \end{array}$$

φ es un automorfismo de $\mathbf{Q}(\mathbf{i})$:

$$\begin{array}{l} \varphi[(a+b\mathbf{i}) + (c+d\mathbf{i})] = f[(a+c) + (b+d)\mathbf{i}] = (a+c) - (b+d)\mathbf{i} \\ = (a - b\mathbf{i}) + (c - d\mathbf{i}) = f(a + b\mathbf{i}) + f(c + d\mathbf{i}) \\ \varphi[(a+b\mathbf{i})(c+d\mathbf{i})] = f[(ac - bd) + (ad + bc)\mathbf{i}] = (ac - bd) - (ad + bc)\mathbf{i} \\ = (a - b\mathbf{i})(c - d\mathbf{i}) = f(a + b\mathbf{i})f(c + d\mathbf{i}) \\ 0 = f(a + b\mathbf{i}) = a - b\mathbf{i} \to\ a + bi = 0. \end{array}$$

Recíprocamente, si $f \in \mathcal{G}(\mathbf{Q}(\mathbf{i}))\backslash\{1_{\mathbf{Q}(\mathbf{i})}\}$, veamos que $f = \varphi$. Para ello, antes notemos que, si E es una extensión de F y $h \in \mathcal{G}(E)$, entonces $h_{|F} \in \mathcal{G}(F)$. Por lo tanto, $f_{|\mathbf{Q}} \in \mathcal{G}(\mathbf{Q})$. Como vimos anteriormente que $\mathcal{G}(\mathbf{Q})$ es un grupo trivial, tenemos que

$$\forall\ a \in \mathbf{Q}, \quad f(a) = a\ .$$

Así

$$f(\mathbf{i})^2 = f(\mathbf{i}^2) = f(-1) = -1 \Rightarrow f(\mathbf{i}) \in \{\pm\mathbf{i}\}$$

y distinguimos dos casos

Uno. $f(\mathbf{i}) = \mathbf{i}$. Entonces, dado $a + b\mathbf{i} \in \mathbf{Q}(\mathbf{i})$

$$f(a+b\mathbf{i}) = f(a) + f(b)f(\mathbf{i}) = a + b\mathbf{i} \Rightarrow f = 1_{\mathbf{Q}(\mathbf{i})}. \text{ Absurdo.}$$

Dos. $f(\mathbf{i}) = -\mathbf{i}$. Entonces, dado $a + b\mathbf{i} \in \mathbf{Q}(\mathbf{i})$

$$f(a+b\mathbf{i}) = f(a) + f(b)f(\mathbf{i}) = a - b\mathbf{i} \Rightarrow f = \varphi.$$

De manera totalmente análoga a lo hecho antes se demuestra que $\mathcal{G}(\mathbf{Q}(\sqrt{2})) = \{1_{\mathbf{Q}(\sqrt{2})}, \psi\}$, siendo

$$\begin{array}{rcl} \psi & : & \mathbf{Q}(\sqrt{2}) \longrightarrow \mathbf{Q}(\sqrt{2}) \\ & & a + b\sqrt{2} \rightarrow a - b\sqrt{2}. \clubsuit \end{array}$$

Ex. 226 *Si* $\zeta = \mathrm{e}^{\frac{2\pi\mathbf{i}}{p}}$, *p primo, demostrar que* $\mathcal{G}(\mathbf{Q}(\zeta))$ *es isomorfo al grupo* $\mathbf{Z}'_p$.

$\equiv$

Recordemos que el grupo $\mathbf{Z}'_p$ se refiere al grupo multiplicativo $\{1, 2, ..., p-1\}$. Así, definimos

$$\begin{array}{rcl} \psi & : & \mathcal{G}(\mathbf{Q}(\zeta)) \longrightarrow \mathbf{Z}'_p \\ & & f \rightarrow \psi(f) := k \ / \ \mathrm{e}^{\frac{2\pi k\mathbf{i}}{p}} = f(\zeta). \end{array}$$

ψ bien definida: Dado $f \in \mathcal{G}(\mathbf{Q}(\zeta))$, vimos antes que, si $a \in \mathbf{Q}$, entonces $f(a) = a$. Así

$$f(\zeta)^p = f(\zeta^p) = f(1) = 1 \Rightarrow f(\zeta) \text{ es raiz p} - \text{ésima de la unidad.}$$

Por tanto, como $f(\zeta) \neq 1$, tenemos que

$$f(\zeta) \in \{ \mathrm{e}^{\frac{2\pi\mathbf{i}}{p}}, \mathrm{e}^{\frac{2\cdot 2\pi\mathbf{i}}{p}}, ..., \mathrm{e}^{\frac{2(p-1)\pi\mathbf{i}}{p}} \},$$

por lo que existe $k \in \{1, 2, ..., p-1\}$ tal que $f(\zeta) = \mathrm{e}^{\frac{2k\pi\mathbf{i}}{p}}$.

ψ homomorfismo de grupos: Si $f, g \in \mathcal{G}(\mathbf{Q}(\zeta))$, entonces, fijando

$$\left.\begin{array}{l} r := \psi(f \circ g) \\ k := \psi(f) \\ q := \psi(g) \end{array}\right\} \Rightarrow \left\{\begin{array}{l} (f \circ g)(\zeta) = \mathrm{e}^{\frac{2\pi r\mathbf{i}}{p}} \\ f(\zeta) = \mathrm{e}^{\frac{2\pi k\mathbf{i}}{p}} \\ g(\zeta) = \mathrm{e}^{\frac{2\pi q\mathbf{i}}{p}} \end{array}\right\}$$

$$\Rightarrow \mathrm{e}^{\frac{2\pi r\mathbf{i}}{p}} = (f \circ g)(\zeta) = f(\mathrm{e}^{\frac{2\pi q\mathbf{i}}{p}}) = f(\zeta^q) = f(\zeta)^q = \mathrm{e}^{\frac{2\pi kq\mathbf{i}}{p}}$$

$$\Rightarrow \exists m \in \mathbf{Z} \ / \ \frac{2\pi r\mathbf{i}}{p} - \frac{2\pi kq\mathbf{i}}{p} = 2\pi m\mathbf{i} \Rightarrow p \mid (r - kq).$$

Por tanto, en $\mathbf{Z}'_p$, $r = kq$, i.e., $\psi(f \circ g) = \psi(f)\psi(g)$.

ψ inyectivo: Si $f \in Ker(\psi)$, entonces

$$1 = \psi(f) \ \rightarrow \ f(\zeta) = e^{\frac{2\pi i}{p}} = \zeta \ .$$

Así, si $z \in \mathbf{Q}(\zeta)$, existen $a_0, a_1, ..., a_{p-1} \in \mathbf{Q}$ tales que $z = a_0 + a_1\zeta + ... + a_{p-1}\zeta^{p-1}$ y entonces

$$f(z) = f(a_0+a_1\zeta+...+a_{p-1}\zeta^{p-1}) = a_0+a_1f(\zeta)+...+a_{p-1}f(\zeta^{p-1}) = a_0+a_1\zeta+...+a_{p-1}\zeta^{p-1} = z,$$

lo que implica que f es la identidad.
ψ sobre: Si $k \in \mathbf{Z}'_p$), entonces definimos

$$\begin{array}{rcl} f & : & \mathbf{Q}(\zeta) \longrightarrow \mathbf{Q}(\zeta) \\ & & \sum_{j=0}^{p-1} a_j\zeta^j \rightarrow \sum_{j=0}^{p-1} a_j\zeta^{kj}. \end{array}$$

Veamos que f es un automorfismo de $\mathbf{Q}(\zeta)$: Dados $z_1 = \sum_{j=0}^{p-1} a_j\zeta^j$, $z_2 = \sum_{j=0}^{p-1} b_j\zeta^j \in \mathbf{Q}(\zeta)$

$$\begin{array}{l} f(z_1 + z_2) = f[(\sum_{j=0}^{p-1} a_j\zeta^j) + (\sum_{j=0}^{p-1} b_j\zeta^j)] = f(\sum_{j=0}^{p-1}(a_j + b_j)\zeta^j \\ = \sum_{j=0}^{p-1}(a_j + b_j)\zeta^{kj} = (\sum_{j=0}^{p-1} a_j\zeta^{kj}) + (\sum_{j=0}^{p-1} b_j\zeta^{kj}) = f(z_1) + f(z_2). \\ f(z_1z_2) = f[(\sum_{j=0}^{p-1} a_j\zeta^j)(\sum_{j=0}^{p-1} b_j\zeta^j)] = f(\sum_{i,j=0}^{p-1}(a_ib_j)\zeta^{i+j}) \\ = \sum_{i,j=0}^{p-1}(a_ib_j)\zeta^{k(i+j)} = (\sum_{i=0}^{p-1} a_i\zeta^{ki})(\sum_{j=0}^{p-1} b_j\zeta^{kj}) = f(z_1)f(z_2). \end{array}$$

Para ver que f es inyectivo, sea $z = \sum_{j=0}^{p-1} a_j\zeta^j \in Ker(f)$. Entonces, como, al ser p primo, k (suponiendo que $k \neq 1$, de lo contrario, todo es obvio) tiene orden $p-1$ en el grupo multiplicativo $\mathbf{Z}'_p$, se tiene que $\{1, k, k^2, ..., k^{p-2}\} = \{1, 2, ..., p-1\}$ y

$$0 = f(z) = f(\sum_{j=0}^{p-1} a_j\zeta^j) = \sum_{j=0}^{p-1} a_j\zeta^{kj} \ \rightarrow \ a_0 = a_1 = ... = a_{p-1} \rightarrow \ z = 0.$$

Para ver que f es sobre, sea $\omega = \sum_{j=0}^{p-1} b_j\zeta^j \in \mathbf{Q}(\zeta)$. Para cada $j = 0, 1, ..., p-1$, existe $i(j) \in \{0, 1, ..., p-1\}$ tal que $k^{i(j)} = j$. Entonces, tomando $z := \sum_{j=0}^{p-1} b_j\zeta^{i(j)}$, tenemos

$$\omega = \sum_{j=0}^{p-1} b_j\zeta^j = \sum_{j=0}^{p-1} b_j\zeta^{k^{i(j)}} = f(\sum_{j=0}^{p-1} b_j\zeta^{i(j)}) = f(z).$$

Finalmente, nos queda ver que $\psi(f) = k$, lo cual es muy fácil:

$$e^{\frac{2\pi ki}{p}} \ = \ f(\zeta) \ \Rightarrow \ \psi(f) = k. \ \clubsuit$$

Ex. 227 *Sea E un cuerpo y $\Phi \in \mathcal{G}(E)$. Demostrar que $F = \{ \alpha \in E \ : \ \Phi(\alpha) = \alpha\}$ es un subcuerpo de E (el cuerpo fijo de Φ).*

$\equiv$

Para demostrar que un subconjunto F de un cuerpo E es subcuerpo, todo se reduce a verificar que $(F,+)$ es subgrupo de $(E,+)$ y que $(F^*,\cdot)$ es subgrupo de $(E^*,\cdot)$. Para ello, dados $\alpha,\beta \in F$

$$\Phi(\alpha-\beta)=\Phi(\alpha)-\Phi(\beta)=\alpha-\beta \;\rightarrow\; \alpha-\beta\in F$$

$$\text{Si } \alpha,\beta\in F^*,\ \Phi(\alpha\cdot\beta^{-1})=\Phi(\alpha)\Phi(\beta)^{-1}=\alpha\cdot\beta^{-1} \;\rightarrow\; \alpha\cdot\beta^{-1}\in F^*. \ \clubsuit$$

Ex. 228 *Sea E un cuerpo finito de característica p.*

a) Demostrar que $\begin{array}{rcl}\Phi: & E & \longrightarrow E \\ & \alpha & \rightarrow \Phi(\alpha)=\alpha^p\end{array}$ *es un automorfismo.*

b) Indicar qué condiciones se han de cumplir para que Φ sea automorfismo cuando E es infinito.

$\equiv$

a) Dados $\alpha,\beta\in E$, como $p=carac(E)$ es primo,

$$\left.\begin{array}{l}\Phi(\alpha+\beta)=(\alpha+\beta)^p=\alpha^p+\beta^p=\Phi(\alpha)+\Phi(\beta)\\ \Phi(\alpha\cdot\beta)=(\alpha\beta)^p=(\alpha)^p\cdot\beta^p=\Phi(\alpha)\cdot\Phi(\beta).\end{array}\right\}\Rightarrow \Phi \text{ es homomorfismo.}$$

Φ inyectivo: Sea $\alpha\in Ker(\Phi)$, entonces

$$0 \;=\; \Phi(\alpha) \;=\; \alpha^p \;\rightarrow\; \alpha=0\ .$$

Al tratarse de una aplicación inyectiva de un conjunto finito en sí mismo, se desprende que Φ es biyectiva.

b) Sea E un cuerpo infinito tal que $carac(E)=p$. Del apartado anterior se deduce que la aplicación Φ (definida como antes) es siempre un homomorfismo inyectivo. Si queremos que Φ sea automorfismo, ha de ser una aplicación sobre, es decir

$$\Phi \text{ automorfismo} \Leftrightarrow\ \forall\alpha\in E,\ \exists\beta\in E\ /\ \alpha=\Phi(\beta)=\beta^p \Leftrightarrow E \text{ es un cuerpo perfecto. } \clubsuit$$

Ex. 229 *Sea $E=F(\alpha)$. Sea $\beta\in E$ una raíz del polinomio mínimo de α sobre F. Demostrar que existe un único automorfismo Φ de E tal que $\Phi(\alpha)=\beta$, y que deja fijo F.*

$\equiv$

Sea $f(x)=a_0+a_1x+...+a_nx^n\in F[x]$ polinomio mínimo de α sobre F tal que $f(\beta)=0$. Sabemos que

$$E \;=\; F(\alpha) \;=\; \{\ \sum_{i=0}^{n-1} c_i\alpha^i \ :\ \ c_i\in F,\ 0\le i\le n-1\ \}.$$

Así, definimos

$$\Phi\ :\ E\ \longrightarrow\ E$$

$$\textstyle\sum_{i=0}^{n-1} c_i\alpha^i \ \rightarrow\ \Phi(\sum_{i=0}^{n-1} c_i\alpha^i) := \sum_{i=0}^{n-1} c_i\beta^i$$

Claramente, $\Phi(\alpha) = \beta$, y, $\forall c \in F$, $\Phi(c) = c$. Veamos que Φ es automorfismo. Dados $g(x), h(x) \in F[x]$ tales que $g(x) = \sum_{i=0}^{n-1} c_i x^i$, $h(x) = \sum_{i=0}^{n-1} d_i x^i$, entonces

$$\Phi[g(\alpha) + h(\alpha)] = \Phi[(g+h)(\alpha)] = (g+h)(\beta) = g(\beta) + h(\beta) = \Phi[g(\alpha)] + \Phi[h(\alpha)]$$

$$\Phi[g(\alpha)h(\alpha)] = \Phi[(gh)(\alpha)] = (gh)(\beta) = g(\beta)h(\beta) = \Phi[g(\alpha)]\Phi[h(\alpha)].$$

Si $g(\alpha) \in Ker(\Phi)$, entonces

$$0 \;=\; \Phi[g(\alpha)] = g(\beta) \;\rightarrow\; \sum_{i=0}^{n-1} c_i \beta^i = 0 \;\rightarrow\; c_i = 0,\; 0 \leq i \leq n-1,$$

ya que, como $f(x)$ es irreducible sobre F y β es raíz de $f(x)$, se tiene que β es un elemento algebraico sobre F del cual $f(x)$ es un polinomio mínimo; por tanto, ningún polinomio de $F[x]$ no nulo de grado menor que n ha de anularse en β. Consecuentemente, tenemos que Φ es un homomorfismo inyectivo. Para ver que también es sobre, observar que Φ puede considerarse, ya que fija F, como una aplicación lineal de E, como espacio vectorial sobre F, en sí mismo. Así, puesto que E es un espacio vectorial de dimensión finita (de hecho, vale $[E : F] = n$), al ser Φ inyectiva se tiene que es automáticamente (teorema del rango) una aplicación sobre. Para acabar el ejercicio, nos falta ver que Φ es el único automorfismo de E que cumple las condiciones del enunciado. Por tanto, sea $\varphi \in \mathcal{G}(E)$ tal que $\varphi(\alpha) = \beta$ y, $\forall c \in F$, $\varphi(c) = c$. Dado $\gamma \in E$, sabemos que existe $g(x) = \sum_{i=0}^{n-1} c_i x^i$ en $F[x]$ tal que $\gamma = g(\alpha)$. Entonces

$$\varphi(\gamma) = \varphi(g(\alpha)) = \varphi(\sum_{i=0}^{n-1} c_i \alpha^i) = \sum_{i=0}^{n-1} \varphi(c_i)\varphi(\alpha^i) = \sum_{i=0}^{n-1} c_i \beta^i$$

$$= g(\beta) = \Phi(g(\alpha)) = \Phi(\gamma);\; \varphi = \Phi. \;\clubsuit$$

Ex. 230 *Sea* $\zeta = \mathrm{e}^{\frac{2\pi \mathrm{i}}{5}}$. *Sea* $\Phi \in \mathcal{G}(\mathbf{Q}(\zeta))$ *tal que* $\Phi(\zeta) = \zeta^4$. *Demostrar que el cuerpo fijo de* Φ *es* $\mathbf{Q}(\sqrt{5})$.

$\equiv$

Recordemos que el cuerpo fijo del automorfismo Φ es

$$F \;:=\; \{\, \alpha \in \mathbf{Q}(\zeta) \;:\; \Phi(\alpha) \;=\; \alpha \,\}.$$

Así pues, veamos que $F = \mathbf{Q}(\sqrt{5})$.
$[\subset]$ Dado $\alpha \in F$, como $\alpha \in \mathbf{Q}(\zeta)$, existen $a, b, c, d \in \mathbf{Q}$ de modo que $\alpha = a + b\zeta + c\zeta^2 + d\zeta^3$, ya que $[\mathbf{Q}(\zeta) : \mathbf{Q}] = 4$ al ser $x^4 + x^3 + x^2 + x + 1$ polinomio mínimo de ζ sobre $\mathbf{Q}$ puesto que ζ es una raíz compleja quinta de la unidad y $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$ con $\zeta \neq 1$. Por tanto, como $\alpha \in F$,

$$\alpha = \Phi(\alpha) \;\rightarrow\; a + b\zeta + c\zeta^2 + d\zeta^3 = a + b\zeta^4 + c\zeta^8 + d\zeta^{12},$$

de lo cual, como $\zeta^5 = 1$,

$$b\zeta+(c-d)\zeta^2+(d-c)\zeta^3-b\zeta^4 = 0 \overset{(\zeta^4=-\zeta^3-\zeta^2-\zeta-1)}{\to} 0 = b(\zeta^3+\zeta^2+2\zeta+1)+(c-d)\zeta^2+(d-c)\zeta^3$$

$$= (b-c+d)\zeta^3 + (b+c-d)\zeta^2 + 2b\zeta + b.$$

Al ser $x^4+x^3+x^2+x+1$ polinomio mínimo de ζ, se deduce que

$$\left.\begin{array}{l} b-c+d=0 \\ b+c-d=0 \\ b=0 \end{array}\right\} \to \left\{\begin{array}{l} b=0 \\ c=d \end{array}\right\} \to \alpha = a + c(\zeta^2+\zeta^3).$$

Llamando $u := \zeta^2+\zeta^3$, tenemos

$$\left.\begin{array}{l} u^2+u-1 = \zeta^4+\zeta^6+2+\zeta^2+\zeta^3-1 = \zeta^4+\zeta^3+\zeta^2+\zeta+1 = 0 \\ u^2+u-1 = (u+\frac{1-\sqrt{5}}{2})(u+\frac{1+\sqrt{5}}{2}) \end{array}\right\} \Rightarrow u \in \{\frac{-1\pm\sqrt{5}}{2}\}.$$

En cualquier caso, $u \in \mathbf{Q}(\sqrt{5})$. Por tanto, $\alpha = a+cu \in \mathbf{Q}(\sqrt{5})$.
[$\supset$] Acabamos de ver que $u = \zeta^2+\zeta \in \{\frac{-1\pm\sqrt{5}}{2}\}$. Por tanto, es evidente que

$$\sqrt{5} \in \{2(\zeta^2+\zeta^3)+1, -2(\zeta^2+\zeta^3)-1\}.$$

Pero

$$\zeta^2+\zeta^3 = \zeta^2+\frac{1}{\zeta^2} = \zeta^2+\overline{\zeta^2} = 2\cdot Re(\zeta^2) = 2\cdot Re[(\cos\frac{2\pi}{5}+\mathbf{i}\sin\frac{2\pi}{5})^2]$$

$$\overset{(De\ Moivre)}{=} 2\cdot Re(\cos\frac{4\pi}{5}+\mathbf{i}\sin\frac{4\pi}{5}) = 2\cdot\cos\frac{4\pi}{5} = 2\cdot\cos\ 144^\circ \in]-1, \cos\ 120^\circ[=]-1, \frac{-1}{2}[.$$

Así,

$$2(\zeta^2+\zeta^3)+1 \in]-1,0[\overset{(\sqrt{5}>0)}{\Rightarrow} \sqrt{5} = -2(\zeta^2+\zeta^3)-1.$$

Entonces

$$\Phi(\sqrt{5}) = \Phi(-2(\zeta^2+\zeta^3)-1) = -2(\zeta^8+\zeta^{12})-1 = -2(\zeta^3+\zeta^2)-1 = \sqrt{5}.$$

Finalmente, si $a+b\sqrt{5} \in \mathbf{Q}(\sqrt{5})$, está claro que $a+b\sqrt{5} \in F$, pues

$$\Phi(a+b\sqrt{5}) = a + b\,\Phi(\sqrt{5}) = a+b\sqrt{5}. \clubsuit$$

Ex. 231 *Sea $\Phi \in \mathcal{G}(E)$ tal que F es su cuerpo fijo. Demostrar que si $\alpha \in E$ es ua raíz de $f(x) \in F[x]$, entonces $\Phi(\alpha)$ es también raíz de $f(x)$.*

$\equiv$

Sea $f(x) = c_0 + c_1x + ... + c_nx^n \in F[x]$. Entonces

$$f[\Phi(\alpha)] = \sum_{i=0}^{n} c_i\Phi(\alpha)^i = \sum_{i=0}^{n} \Phi(c_i)\Phi(\alpha)^i = \Phi(\sum_{i=0}^{n} c_i\alpha^i) = \Phi(0) = 0. \clubsuit$$

Ex. 232 *Sea $\Phi \in \mathcal{G}(E)$ con F de cuerpo fijo. Demostrar que Φ puede extenderse de forma única a una aplicación $\widetilde{\Phi} : E[x] \to E[x]$, con las siguientes propiedades*

a) $\widetilde{\Phi}(c) = \Phi(c), \ \forall c \in E.$

b) $\widetilde{\Phi}(x) = x.$

c) $\forall f(x), g(x) \in E[x], \ \begin{cases} \widetilde{\Phi}[f(x) + g(x)] = \widetilde{\Phi}[f(x)] + \widetilde{\Phi}[g(x)] \\ \widetilde{\Phi}[f(x)g(x)] = \widetilde{\Phi}[f(x)]\widetilde{\Phi}[g(x)]. \end{cases}$

Es decir, $\widetilde{\Phi}$ es un homomorfismo de anillos. Demostrar que el subanillo fijo de $\widetilde{\Phi}$ es $F[x]$.

$\equiv$

Definimos

$$\widetilde{\Phi} \ : \ E[x] \longrightarrow E[x]$$

$$f(x) = \textstyle\sum_{i=0}^{n} c_i x^i \ \to \ \widetilde{\Phi}[f(x)] := \sum_{i=0}^{n} \Phi(c_i) x^i.$$

Está claro que $\widetilde{\Phi}$ está bien definida, pues $\forall c \in E, \ \Phi(c) \in E$. Veamos el cumplimiento de las tres propiedades

a) Si $c \in E$, entonces $\widetilde{\Phi}(c) = \Phi(c)$, de la definición de $\widetilde{\Phi}$.

b) $\widetilde{\Phi}(x) = x$.

c) Dados $f(x) = \sum_{i=0}^{n} c_i x^i, \ g(x) = \sum_{i=0}^{m} d_i x^i$

$$\begin{cases} \widetilde{\Phi}[f(x) + g(x)] = \widetilde{\Phi}(\sum (c_i + d_i) x^i) = \sum \phi(c_i) x^i + \sum \Phi(d_i) x^i = \widetilde{\Phi}[f(x)] + \widetilde{\Phi}[g(x)] \\ \widetilde{\Phi}[f(x)g(x)] \overset{(anàlogo)}{=} \widetilde{\Phi}[f(x)]\widetilde{\Phi}[g(x)]. \end{cases}$$

Veamos la unicidad. Sea $\varphi : E[x] \to E[x]$ una aplicación que cumple las tres condiciones anteriores. Dado $f(x) = \sum_{i=0}^{n} c_i x^i$

$$\varphi(f(x)) \overset{(c)}{=} \sum_{i=0}^{n} \varphi(c_i x^i) \overset{(c)}{=} \sum_{i=0}^{n} \varphi(c_i)\varphi(x^i) \overset{(a,b,c)}{=} \sum_{i=0}^{n} \Phi(c_i) x^i = \widetilde{\Phi}(f(x)).$$

Finalmente, veamos que el conjunto (un dominio de integridad, de hecho) de los elementos fijos de $\widetilde{\Phi}$ es $F[x]$.

$[\subset]$ Si $f(x) = \sum_{i=0}^{n} c_i x^i \in E[x]$ es tal que $\widetilde{\Phi}(f(x)) = f(x)$, entonces

$$f(x) = \sum_{i=0}^{n} c_i x^i = \widetilde{\Phi}(f(x)) = \sum_{i=0}^{n} \Phi(c_i) x^i$$

$$\Rightarrow \ c_i = \Phi(c_i), \ 0 \le i \le n \ \overset{(F \text{ c.f. de } \Phi)}{\Rightarrow} \ c_i \in F, \ 0 \le i \le n.$$

Luego, $f(x) \in F[x]$.

$[\supset]$ Si $f(x) = \sum_{i=0}^{n} c_i x^i \in F[x]$, es evidente que, ya que los coeficientes de $f(x)$ son de F, $\widetilde{\Phi}(f(x)) = f(x)$. ♣

Ex. 233 *Sea $\Phi \in \mathcal{G}(E)$ tal que F es su cuerpo fijo. Sea $f(x) \in E[x]$ un polinomio mónico que se descompone en E. Demostrar que, si $f(x)$ cumple que $\forall \alpha \in E$ tal que $f(\alpha) = 0$ se tiene que $f(\Phi(\alpha)) = 0$, entonces $f(x) \in F[x]$.*

≡

Sean $\lambda_1, \lambda_2, ..., \lambda_n$, posiblemente repetidas, las raíces de $f(x)$ en E de modo que

$$f(x) = (x-\lambda_1)(x-\lambda_2)...(x-\lambda_n).$$

Para cada $i = 1, 2, ..., n$, como $f(\lambda_i) = 0$, tenemos que $f(\Phi(\lambda_i)) = 0$, de manera que $\Phi(\lambda_i)$ es también raíz de $f(x)$. Por tanto, al ser Φ biyectiva,

$$\{\Phi(\lambda_1), \Phi(\lambda_2), ..., \Phi(\lambda_n)\} = \{\lambda_1, \lambda_2, ..., \lambda_n\},$$

de lo que

$$f(x) = (x-\lambda_1)(x-\lambda_2)...(x-\lambda_n) = (x-\Phi(\lambda_1))(x-\Phi(\lambda_2))...(x-\Phi(\lambda_n)).$$

Haciendo uso del ejercicio previo, consideramos la aplicación $\widetilde{\Phi}: E[x] \to E[x]$ allí introducida con las propiedades indicadas. Puesto que el conjunto de elementos fijos de $\widetilde{\Phi}$ es $F[x]$, todo consiste en ver que $\widetilde{\Phi}(f(x)) = f(x)$. Así

$$\widetilde{\Phi}(f(x)) = \widetilde{\Phi}[(x-\lambda_1)(x-\lambda_2)...(x-\lambda_n)] = \widetilde{\Phi}(x-\lambda_1)\widetilde{\Phi}(x-\lambda_2)...\widetilde{\Phi}(x-\lambda_n)$$

$$= (\widetilde{\Phi}(x) - \widetilde{\Phi}(\lambda_1))...(\widetilde{\Phi}(x) - \widetilde{\Phi}(\lambda_n)) = (x-\Phi(\lambda_1))...(x-\Phi(\lambda_n)) = f(x). \clubsuit$$

Ex. 234 *Sea E el cuerpo raíz en $\mathbf{C}$ del polinomio x^4+1.*

a) Hallar automorfismos de E que tengan como cuerpos fijos a $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt{2})$ y $\mathbf{Q}(\sqrt{\mathbf{i}})$.

b) Existe algún automorfismo de E tal que su cuerpo fijo sea $\mathbf{Q}$?

≡

Sea $U_4 := \{\alpha, \beta, \gamma, \delta\}$ el conjunto formado por las cuatro raíces de x^4+1 en $\mathbf{C}$. Al tratarse de raíces cuartas de la unidad, se ve fácilmente que (queda bonito dibujarlas en la circunferencia unidad compleja)

$$\alpha = \frac{\sqrt{2}}{2}(1+\mathbf{i}), \quad \beta = \frac{\sqrt{2}}{2}(-1+\mathbf{i}), \quad \gamma = \frac{\sqrt{2}}{2}(-1-\mathbf{i}), \quad \delta = \frac{\sqrt{2}}{2}(1-\mathbf{i}).$$

Si $\varphi \in \mathcal{G}(E)$, entonces

$$-1 = \varphi(-1) = \varphi(\alpha^4) = \varphi(\alpha)^4 \Rightarrow \varphi(\alpha) \in U_4.$$

Haciendo lo mismo para las demás raíces, deducimos que, al ser φ biyectiva,

$$\varphi(U_4) = U_4.$$

Por tanto, todo automorfismo de E puede ser identificado con un elemento del grupo de las permutaciones de los elementos de U_4. Para verlo más claramente, primero observemos que

$$\beta = \frac{-1}{\alpha}, \quad \gamma = -\alpha, \quad \delta = \frac{1}{\alpha} \Rightarrow E = \mathbf{Q}(\alpha),$$

de donde, si φ es una aplicación de E en sí mismo que fija $\mathbf{Q}$ y conocemos $\varphi(\alpha) \in U_4$, queda claro que φ está ya determinada. Así pues, pasamos a responder a los dos apartados del ejercicio.

a) Consideremos $\varphi, \psi, \Phi \in \mathcal{G}(E)$ tales que

$$\varphi(\alpha) = \beta,\ \psi(\alpha) = \delta,\ \Phi(\alpha) = \gamma \ \Rightarrow \left\{ \begin{array}{l} \varphi(\beta) = \alpha, \varphi(\gamma) = \delta, \varphi(\delta) = \gamma \\ \psi(\beta) = \gamma, \psi(\gamma) = \beta, \psi(\delta) = \alpha \\ \Phi(\beta) = \delta, \varphi(\gamma) = \alpha, \varphi(\delta) = \beta. \end{array} \right.$$

Veamos que, si representamos por $F_\varphi, F_\psi, F_\Phi$ a los cuerpos fijos de φ, ψ y Φ, respectivamente, entonces $F_\varphi = \mathbf{Q}(\sqrt{-2})$, $F_\psi = \mathbf{Q}(\sqrt{2})$ y $F_\Phi = \mathbf{Q}(\sqrt{\mathbf{i}})$.

[$\subset$] Como $F_\varphi, F_\psi, F_\Phi$ están contenidos en $E = \mathbf{Q}(\alpha)$ y $[\mathbf{Q}(\alpha) : \mathbf{Q}] = grado(x^4+1) = 4$, observando además que $\beta^2 = -\mathbf{i} = -\alpha^2$, $\beta^3 = \alpha$, $\beta = \alpha^3$,

$$a+b\alpha+c\alpha^2+d\alpha^3 = \varphi(a+b\alpha+c\alpha^2+d\alpha^3) = a+b\beta+c\beta^2+d\beta^3 \ \rightarrow\ 0 = (b-d)\alpha+2c\alpha^2+(d-b)\alpha^3$$

$$\rightarrow \left\{ \begin{array}{l} c = 0 \\ b = d \end{array} \right\} \rightarrow a+b\alpha+c\alpha^2+d\alpha^3 = a+b(\alpha+\alpha^3) = a+b(\alpha+\beta) = a+b\sqrt{-2} \in \mathbf{Q}(\sqrt{-2}).$$

Para ψ

$$a+b\alpha+c\alpha^2+d\alpha^3 = \psi(a+b\alpha+c\alpha^2+d\alpha^3) = a+b\delta+c\delta^2+d\delta^3 = a-b\beta+c\beta^2-d\beta^3$$

$$\rightarrow\ 0 = (b+d)\alpha+2c\alpha^2+(d+b)\alpha^3 \ \rightarrow \left\{ \begin{array}{l} c = 0 \\ b = -d \end{array} \right\} \rightarrow a+b\alpha+c\alpha^2+d\alpha^3$$

$$= a+b(\alpha-\alpha^3) = a+b(\alpha-\beta) = a+b\sqrt{2} \in \mathbf{Q}(\sqrt{2}).$$

Para Φ

$$a+b\alpha+c\alpha^2+d\alpha^3 = \Phi(a+b\alpha+c\alpha^2+d\alpha^3) = a+b\gamma+c\gamma^2+d\gamma^3 = a-b\alpha+c\alpha^2-d\alpha^3$$

$$\rightarrow\ 0 = 2b\alpha+2d\alpha^3$$

$$\rightarrow \left\{ \begin{array}{l} b = 0 \\ d = 0 \end{array} \right\} \rightarrow\ \ a+b\alpha+c\alpha^2+d\alpha^3 == a+c\alpha^2 = a+c\mathbf{i} \in \mathbf{Q}(\mathbf{i}).$$

[$\supset$] Como $\sqrt{-2} = \mathbf{i}\sqrt{2} = \alpha+\beta$, $\sqrt{2} = \alpha-\beta$ y $\mathbf{i} = \alpha^2$, es obvio que

$$\mathbf{Q}(\sqrt{-2}) \ \subset\ F_\varphi,\ \mathbf{Q}(\sqrt{2}) \ \subset\ F_\psi,\ \ \mathbf{Q}(\mathbf{i}) \ \subset\ F_\Phi.$$

b) Veamos que no existen automorfismos de E cuyo cuerpo fijo sea exactamente $\mathbf{Q}$:

Sea $\eta \in \mathcal{G}(E)$ y sea F_η su cuerpo fijo. Entonces, como $\eta(\alpha) \in U_4$, tenemos cuatro posibilidades

Una. $\eta(\alpha) = \alpha$. Claramente $\alpha \in F_\eta$, de lo que $F_\eta \neq \mathbf{Q}$.

Dos. $\eta(\alpha) = \beta$. Entonces, $\eta = \varphi$, siendo φ el automorfismo considerado en el apartado anterior. Así, $F_\eta = F_\varphi = \mathbf{Q}(\sqrt{-2}) \neq \mathbf{Q}$.

Tres. $\eta(\alpha) = \gamma$. Entonces, $\eta = \Phi$, siendo Φ el automorfismo considerado en el apartado anterior. Así, $F_\eta = F_\Phi = \mathbf{Q}(\mathbf{i}) \neq \mathbf{Q}$.

Cuatro. $\eta(\alpha) = \delta$. Entonces, $\eta = \psi$, siendo ψ el automorfismo considerado en el apartado anterior. Así, $F_\eta = F_\psi = \mathbf{Q}(\sqrt{2}) \neq \mathbf{Q}$. ♣

Ex. 235 *Sea E el cuerpo raíz en $\mathbf{C}$ del polinomio x^4+1 sobre $\mathbf{Q}$. Demostrar que $[E:\mathbf{Q}]=4$.*

$\equiv$

Del ejercicio anterior, llamando como allí $U_4=\{\alpha,\beta,\gamma,\delta\}$ al conjunto de las cuatro raíces cuartas complejas de la unidad, sabemos que, puesto que
$x^4+1=(x-\alpha)(x-\beta)(x-\gamma)(x-\delta)$ es el polinomio mínimo de α sobre $\mathbf{Q}$,

$$E \;=\; \mathbf{Q}(\alpha) \;\Rightarrow\; [E:\mathbf{Q}] \;=\; grado(x^4+1) \;=\; 4,$$

sin embargo, vamos a resolver este ejercicio de otra forma. En concreto, aplicando un resultado que dice: *Sea E es una extensión de F y sea, para cada $\varphi\in\mathcal{G}(E)$, F_φ el cuerpo fijo de φ. Si se cumple que $\cap_{\varphi\in\mathcal{G}(E)}F_\varphi=F$, entonces $[E:F]=o(\mathcal{G}(E))$.*

Vimos en el anterior ejercicio que $\mathcal{G}(E)=\{1_E,\varphi,\psi,\Phi\}$, donde cada uno de estos automorfismos se identifica con las siguientes permutaciones de U_4

$$\begin{array}{l} 1_E \;\equiv\; Id_{U_4} \\ \varphi \;\equiv\; (\alpha\beta)(\gamma\delta) \\ \psi \;\equiv\; (\alpha\delta)(\beta\gamma) \\ \Phi \;\equiv\; (\alpha\gamma)(\beta\delta). \end{array} \qquad \text{[Notar que } \mathcal{G}\text{(E) es el Viergruppe]}$$

Así pues, en virtud del resultado teórico indicado, todo se reduce a demostrar que

$$F_{1_E} \;\cap\; F_\varphi \;\cap\; F_\psi \;\cap\; F_\Phi \;=\; \mathbf{Q}.$$

En efecto, de lo realizado en el ejercicio previo

$$F_{1_E} \;\cap\; F_\varphi \;\cap\; F_\psi \;\cap\; F_\Phi \;=\; E \;\cap\; \mathbf{Q}(\sqrt{-2}) \;\cap\; \mathbf{Q}(\sqrt{2}) \;\cap\; \mathbf{Q}(\sqrt{\mathbf{i}}) \;=\mathbf{Q},$$

como vemos seguidamente: Al ser elemental que $\mathbf{Q}$ está contenido en los cuatro cuerpos fijos anteriores, veamos que $E\cap\mathbf{Q}(\sqrt{-2})\cap\mathbf{Q}(\sqrt{2})\cap\mathbf{Q}(\sqrt{\mathbf{i}}) \;\subset\mathbf{Q}$. De hecho, vamos a demostrar que $\mathbf{Q}(\sqrt{2})\cap\mathbf{Q}(\sqrt{\mathbf{i}}) \;\subset\mathbf{Q}$. Sea $\lambda\in\mathbf{Q}(\sqrt{2})\cap\mathbf{Q}(\sqrt{\mathbf{i}})$, entonces

$$\exists a,b,c,d\in\mathbf{Q}\;/\;\left\{\begin{array}{l}\lambda=a+b\sqrt{2}\\ \lambda=c+d\mathbf{i}\end{array}\right\}\;\rightarrow\; a-c+b\sqrt{2}-d\mathbf{i}=0$$

$$\rightarrow\left\{\begin{array}{l}a-c+b\sqrt{2}=0\\ d=0\end{array}\right.\rightarrow\left\{\begin{array}{l}a-c=0\rightarrow\; a=c\\ b=0\end{array}\right\}\;\Rightarrow\;\lambda\;=\;a\;\in\;\mathbf{Q}.\;\clubsuit$$

Ex. 236 *Sea $\zeta=\mathrm{e}^{\frac{2\pi\mathbf{i}}{5}}$.*

a) Hallar un grupo de automorfismos de $\mathbf{Q}(\zeta)$ cuyo cuerpo fijo sea $\mathbf{Q}$.

b) Calcular $[\mathbf{Q}(\zeta):\mathbf{Q}]$.

≡

a) Observemos primero que $\zeta = e^{\frac{2\pi i}{5}}$ es una raíz quinta compleja de la unidad, ya que $\zeta^5 = 1$. Lo que desea el ejercicio es que encontremos un subgrupo $H \subset \mathcal{G}(\mathbf{Q}(\zeta))$ tal que $\cap_{\varphi \in H} F_\varphi = \mathbf{Q}$. Así, representando por $U := \{\zeta, \zeta^2, \zeta^3, \zeta^4\}$ al conjunto de las raíces quintas de la unidad distintas de 1, claramente tenemos que, si φ es un automorfismo de $\mathbf{Q}(\zeta)$, entonces $\varphi(U) = U$. Por tanto, los automorfismos de $\mathbf{Q}(\zeta)$ se identifican con un subgrupo del grupo de las permutaciones del conjunto U, de modo que $\mathcal{G}(\mathbf{Q}(\zeta))$ tiene exactamente 4 elementos según la imagen que se asigne a ζ

$$\left.\begin{array}{l} \text{Si } \Phi_1(\zeta) = \zeta \ \to \ \Phi_1 \equiv Id_U \\ \text{Si } \Phi_2(\zeta) = \zeta^2 \ \to \ \Phi_2 \equiv (\zeta\zeta^2\zeta^4\zeta^3) \\ \text{Si } \Phi_3(\zeta) = \zeta^3 \ \to \ \Phi_3 \equiv (\zeta\zeta^3\zeta^4\zeta^2) \\ \text{Si } \Phi_4(\zeta) = \zeta^4 \ \to \ \Phi_4 \equiv (\zeta\zeta^4)(\zeta^2\zeta^3) \end{array}\right\} \Rightarrow \mathcal{G}(\mathbf{Q}(\zeta)) = \{\Phi_1, \Phi_2, \Phi_3, \Phi_4\}.$$

Todo consiste pues en ver que $F_{\Phi_1} \cap F_{\Phi_2} \cap F_{\Phi_3} \cap F_{\Phi_4} = \mathbf{Q}$. De un ejercicio resuelto anes, sabemos que $F_{\Phi_4} = \mathbf{Q}(\sqrt{5})$, por lo tanto demostrando que $\Phi_2(\sqrt{5}) \neq \sqrt{5}$ habremos terminado, ya que

$$F_{\Phi_1} \cap F_{\Phi_2} \cap F_{\Phi_3} \cap F_{\Phi_4} \ \subset \ F_{\Phi_2} \cap F_{\Phi_4} \ = \ F_{\Phi_2} \cap \mathbf{Q}(\sqrt{5}) \ = \ \mathbf{Q}.$$

En efecto, como $\sqrt{5} \in \mathbf{Q}(\zeta)$, existen $a, b, c, d, e \in \mathbf{Q}$ tales que $\sqrt{5} = a + b\zeta + c\zeta^2 + d\zeta^3 + e\zeta^4$ y entonces, suponiendo que $\Phi_2(\sqrt{5}) = \sqrt{5}$,

$$a + b\zeta + c\zeta^2 + d\zeta^3 + e\zeta^4 = \Phi_2(\sqrt{5}) \ = \ a + b\zeta^2 + c\zeta^4 + d\zeta + e\zeta^3,$$

de donde

$$(b-d)\zeta + (c-b)\zeta^2 + (d-e)\zeta^3 + (e-c)\zeta^4 = 0 \to b = c = d = e$$

$$\to \sqrt{5} = a + b(\zeta + \zeta^2 + \zeta^3 + \zeta^4) = a - b,$$

lo que es absurdo.

b) Como consecuencia del apartado anterior, $[\mathbf{Q}(\zeta) : \mathbf{Q}] = o(\mathcal{G}(\mathbf{Q}(\zeta)) = 4$. Observar que otra forma más directa de ver lo anterior consiste en, sabiendo que $x^4 + x^3 + x^2 + x + 1$ es polinomio mínimo de ζ sobre $\mathbf{Q}$, entonces $[\mathbf{Q}(\zeta) : \mathbf{Q}] = 4$. ♣

Ex. 237 *Sea E el cuerpo raíz en $\mathbf{C}$ de $x^3 - 2$ sobre $\mathbf{Q}$. Hallar un grupo de 6 automorfismos de E tal que su cuerpo fijo sea $\mathbf{Q}$, demostrando con ello que $[E : \mathbf{Q}] = 6$.*

≡

Factorizando el polinomio $x^3 - 2$ en $\mathbf{C}$

$$x^3 \ - \ 2 \ = \ (x - \sqrt[3]{2})[x - \frac{\sqrt[3]{2}}{2}(-1 + \mathbf{i}\sqrt{3})][x - \frac{\sqrt[3]{2}}{2}(-1 - \mathbf{i}\sqrt{3})].$$

Si llamamos $\alpha := \sqrt[3]{2}$, $\beta := \frac{\sqrt[3]{2}}{2}(-1 + \mathbf{i}\sqrt{3})$, entonces

$$E = \mathbf{Q}(\alpha, \beta, \overline{\beta}) \ \overset{(\overline{\beta} = -\alpha - \beta)}{=} \ \mathbf{Q}(\alpha, \beta).$$

Si $\varphi \in \mathcal{G}(E)$ ha de fijar $\mathbf{Q}$, entonces

$$\varphi(\alpha)^3 - 2 \;=\; \varphi(\alpha^3 - 2) \;=\; \varphi(0) \;=\; 0,$$

de donde, haciendo lo mismo para las otras raíces $\beta, \overline{\beta}$, tenemos que $\varphi(\{\alpha, \beta, \overline{\beta}\}) = \{\alpha, \beta, \overline{\beta}\}$, es decir, podemos considerar los automorfismos de E que fijan $\mathbf{Q}$ como permutaciones del conjunto de las raíces $\{\alpha, \beta, \overline{\beta}\}$. Por tanto, como el grupo simétrico Σ_3 consta de 6 elementos, tenemos que los automorfismos de E que fijan $\mathbf{Q}$ son

α	β	$\overline{\beta}$	Automorfismo
α	β	$\overline{\beta}$	$\varphi_1 \equiv Id$
α	$\overline{\beta}$	β	φ_2
β	α	$\overline{\beta}$	φ_3
β	$\overline{\beta}$	α	φ_4
$\overline{\beta}$	β	α	φ_5
$\overline{\beta}$	α	β	φ_6 .

Así, llamando $G := \{\, \varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6\}$, tenemos que G es un grupo de automorfismos de E y sólo falta ver que $F_{\varphi_1} \cap F_{\varphi_2} \cap F_{\varphi_3} \cap F_{\varphi_4} \cap F_{\varphi_5} \cap F_{\varphi_6} = \mathbf{Q}$. Para ello, primero vemos que $F_{\varphi_2} = \mathbf{Q}(\alpha)$.

$[\supset]$ $\mathbf{Q}$ está fijado por cualquier automorfismo de un cuerpo numérico. Además, de la definición de φ_2, $\varphi_2(\alpha) = \alpha$ implica que $\alpha \in F_{\varphi_2}$.

$[\subset]$ Si $\lambda \in F_{\varphi_2} \subset E = \mathbf{Q}(\alpha, \beta)$, como el conjunto $\{1, \alpha, \beta, \alpha^2, \beta^2, \alpha\beta\}$ forma un sistema generador de E sobre $\mathbf{Q}$, existen $a, b, c, d, e, f \in \mathbf{Q}$ tales que $\lambda = a + b\alpha + c\beta + d\alpha^2 + e\beta^2 + f\alpha\beta$. Entonces

$$\lambda = \varphi_2(\lambda) \;\Rightarrow\; a + b\alpha + c\beta + d\alpha^2 + e\beta^2 + f\alpha\beta = a + b\alpha + c\overline{\beta} + d\alpha^2 + e\overline{\beta}^2 + f\alpha\overline{\beta},$$

de donde

$$c(\beta - \overline{\beta}) + e(\beta^2 - \overline{\beta}^2) + f\alpha(\beta - \overline{\beta}) = 0 \;\rightarrow\; c + e(\beta + \overline{\beta}) + f\alpha = 0 \rightarrow\; c + (e - f)\alpha = 0,$$

entonces

$$\left.\begin{array}{l} c = 0 \\ e = f \end{array}\right\} \;\rightarrow\; \lambda = a + b\alpha + d\alpha^2 + e\beta(\beta + \alpha) = a + b\alpha + (d - e)\alpha^2 \in \mathbf{Q}(\alpha).$$

Finalmente

$$F_{\varphi_1} \cap F_{\varphi_2} \cap F_{\varphi_3} \cap F_{\varphi_4} \cap F_{\varphi_5} \cap F_{\varphi_6} \;\subset\; F_{\varphi_2} \cap F_{\varphi_3} \;=\; \mathbf{Q}(\alpha) \cap F_{\varphi_3},$$

por lo que todo se reduce a probar que $\mathbf{Q}(\alpha) \cap F_{\varphi_3} \;\subset\; \mathbf{Q}$. Si $\lambda \in \mathbf{Q}(\alpha) \cap F_{\varphi_3}$, entonces existen $a, b, c \in \mathbf{Q}$ tales que

$$\lambda = a + b\alpha + c\alpha^2 \;\Rightarrow\; a + b\alpha + c\alpha^2 = \varphi_3(a + b\alpha + c\alpha^2) = a + b\beta + c\beta^2,$$

así

$$0 = b(\alpha - \beta) + c(\alpha^2 - \beta^2) \;\rightarrow\; 0 = b + c(\alpha + \beta) = b - c\overline{\beta} \;\rightarrow \left\{\begin{array}{l} b = 0 \\ c = 0 \end{array}\right\} \rightarrow\; \lambda = a \in \mathbf{Q}. \;\clubsuit$$

3.2. Extensiones de Galois

Ex. 238

a) Sea F un cuerpo de característica distinta de 2. Sea E una extensión de F tal que $[E:F]=2$. Demostrar que E es una extensión de Galois de F.

b) Si $carac(F)=2$, puede tener F una extensión de Galois de grado 2 ?

≡

Recordemos primero que E es una extensión de Galois de F siempre que sea una extensión finita normal y separable , i.e., E es el cuerpo raíz de un polinomio de $F[x]$ que se descompone totalmente en factores lineales distintos. Un teorema de E. Artin establece lo siguiente: *Si E es una extensión finita de F, son equivalentes*

a) E es una extensión de Galois de F.

b) E es el cuerpo raíz de un polinomio separable de $F[x]$.

c) $[E:F]=o(G(E/F))$, donde $G(E/F)$ es el grupo de los automorfismos de E cuyo cuerpo fijo es F. Este grupo de automorfismos recibe el nombre de grupo de Galois de E sobre F y se representa como $Gal(E/F)$.

a) Como $[E:F]=2$, existe $\alpha\in E$ tal que $E=F(\alpha)$. Además, existe un polinomio $f(x)=x^2+rx+s\in F[x]$ que es polinomio mínimo de α sobre F. Definimos la siguiente aplicación

$$\begin{array}{rcl}\varphi & : & E \longrightarrow E \\ & & a+b\alpha \ \rightarrow \ \varphi(a+b\alpha):=a-b(r+\alpha)\end{array}$$

Claramente φ está bien definida. Veamos que es un automorfismo

$$\varphi[(a+b\alpha)+(c+d\alpha)]=\varphi[(a+c)+(b+d)\alpha]=(a+c)-(b+d)(r+\alpha)=[a-b(r+\alpha)]+[c-d(r+\alpha)]$$

$$=\ \varphi(a+b\alpha)+\varphi(c+d\alpha).$$

$$\varphi[(a+b\alpha)(c+d\alpha)]=\varphi[(ac)+(ad+bc)\alpha+bd\alpha^2]\ =\ (*)$$

ahora, como $\alpha^2=-r\alpha-s$, siguiendo de $(*)$

$$(*)\ =\ \varphi[(ac)+(ad+bc)\alpha+bd(-r\alpha-s)]=\varphi[(ac-bds)+(ad+bc-bdr)\alpha]$$

$$=(ac-bds)-(ad+bc-bdr)(r+\alpha)=\ ac-bds-adr-bcr+bdr^2-(ad+bc-bdr)\alpha.$$

Por otra parte

$$\varphi(a+b\alpha)\varphi(c+d\alpha)=[a-b(r+\alpha)][c-d(r+\alpha)]=ac-ad(r+\alpha)-bc(r+\alpha)+bd(r+\alpha)^2$$

$$=\ ac-adr-bcr+(-ad-bc)\alpha+bd(r^2+2r\alpha+\alpha^2)$$

$$=ac-adr-bcr+(-ad-bc)\alpha+bd(r^2+2r\alpha-r\alpha-s)$$

$$=ac-adr-bcr+(-ad-bc)\alpha+bd(r^2+r\alpha-s)=ac-adr-bcr+bdr^2-bds+(-ad-bc+bdr)\alpha,$$

que coincide con el resultado obtenido arriba. Veamos que φ es inyectiva: Sea $a+b\alpha \in E$ tal que $\varphi(a+b\alpha)=0$, entonces

$$0 \;=\; \varphi(a+b\alpha) \;=\; a-b(r+\alpha) \;=\; a-br-b\alpha \;\to\; \left\{ \begin{array}{l} a-br=0 \\ b=0 \to\; a=0 \end{array} \right\} \;\Rightarrow\; a+b\alpha=0.$$

Ahora vemos que φ es sobre: Dado $a+b\alpha \in E$, nos planteamos la ecuación

$$a+b\alpha=\varphi(x+y\alpha)=x-y(r+\alpha)=x-yr-y\alpha \;\to\; \left\{ \begin{array}{l} a=x-yr \\ b=-y \end{array} \right\} \;\to\; \left\{ \begin{array}{l} y=-b \\ x=a-br, \end{array} \right.$$

es decir, $\varphi[(a-br)-b\alpha]=a+b\alpha$.

Seguidamente, comprobamos que $G:=\{1_E,\varphi\}$ es subgrupo de $\mathcal{G}(E)$. Para ello no hay más que verificar que $\varphi^2=1_E$: Si $a+b\alpha \in E$

$$\varphi^2(a+b\alpha) \;=\; \varphi[a-b(r+\alpha)]=\varphi[(a-br)-b\alpha]=(a-br)+b(r+\alpha)=a+b\alpha.$$

Ahora demostramos que F es el cuerpo fijo de G, es decir, que $F_\varphi=F$: Si $a \in F$, es evidente que $\varphi(a)=\varphi(a+0\cdot\alpha)=a$, i.e., $F_\varphi \supset F$. Recíprocamente, si $a+b\alpha \in F_\varphi$, entonces

$$a+b\alpha=\varphi(a+b\alpha)=a-b(r+\alpha)=a-br-b\alpha \to \left\{ \begin{array}{l} a=a-br \\ b=-b \end{array} \right\}$$

$$\stackrel{(caract(F)\neq 2)}{\to} b=0 \to a+b\alpha=a \in F.$$

Como ya hemos demostrado que E es una extensión normal de F, para terminar sólo nos falta ver que E es una extensión separable. Pero éso es obvio ya que $E=F(\alpha)$ es el cuerpo raíz de α. Por lo tanto, E es una extensión de Galois de F.

b) Veamos con un ejemplo que existen extensiones de Galois E de cuerpos F con $caract(F)=2$ tales que $[E:F]=2$.

Tomamos $F:=\mathbf{Z}_2=\{0,1\}$. En este cuerpo el polinomio x^2+x+1 no tiene raíces, por lo que, considerando α como una raíz de dicho polinomio en alguna extensión de F, sea $E:=\mathbf{Z}_2(\alpha)$. Claramente, E es una extensión de F, de hecho

$$E \;=\; \{a+b\alpha \;:\; a,b \in \mathbf{Z}_2\} \;=\; \{\,0,\;1,\;\alpha,\;1+\alpha\,\}.$$

Aplicando el Teorema de Artin, para ver que E es extensión de Galois de F, veamos que existe un automorfismo φ de E cuyo cuerpo fijo es F y tal que $G:=\{1_E,\varphi\}=Gal(E/F)$. Para ello, como $\varphi(\alpha)$ ha de ser raíz de x^2+x+1 $(\varphi(\alpha)^2+\varphi(\alpha)+1=\varphi(\alpha^2+\alpha+1)=\varphi(0)=0)$, y como $\varphi \neq 1_E$, está claro que $\varphi(\alpha)=1+\alpha$. Por tanto, el automorfismo φ es

$$\varphi(a+b\alpha) \;=\; a \;+\; b\,\varphi(\alpha) \;=\; a+b(1+\alpha) \;=\; a+b+b\alpha.$$

Es immediato comprobar que φ es homomorfismo de cuerpos. Además, $0=\varphi(a+b\alpha)=a+b+b\alpha \;\to\; a=b=0 \to\; a+b\alpha=0$, lo que prueba que es inyectivo. Al tratarse de una aplicación inyectiva de un conjunto finito en sí mismo, φ es biyectiva. Finalmente, si $a+b\alpha=\varphi(a+b\alpha)=a+b+b\alpha \;\to\; b=0 \to\; a+b\alpha=a \in F$, lo que demuestra que F es el cuerpo fijo de φ. ♣

Ex. 239 *Sea* $\zeta = e^{\frac{2\pi i}{5}}$. *Deducir que* $\mathbf{Q}(\zeta)$ *es una extensión de Galois de* $\mathbf{Q}$

$\equiv$

$\mathbf{Q}(\zeta)$ es una extensión finita de $\mathbf{Q}$ tal que es el cuerpo raíz del polinomio $x^4+x^3+x^2+x+1 \in \mathbf{Q}[x]$, que es separable pues $x^4+x^3+x^2+x+1 = (x-\zeta)(x-\zeta^2)(x-\zeta^3)(x-\zeta^4)$. Del teorema de Artin, $\mathbf{Q}(\zeta)$ es una extensión de Galois de $\mathbf{Q}$. Observar que también se podría haber demostrado haciendo uso de la condición equivalente tercera del teorema de Artin, ya que en un ejercicio anterior se vió que $G(\mathbf{Q}(\zeta)/\mathbf{Q}) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$, donde $\varphi_i(\zeta) = \zeta^i$, $1 \leq i \leq 4$, por lo que

$$[\mathbf{Q}(\zeta) : \mathbf{Q}] \;=\; grado(x^4+x^3+x^2+x+1) \;=\; 4 \;=\; o(\mathbf{Q}(\zeta)/\mathbf{Q}). \;\clubsuit$$

Ex. 240

a) Demostrar que $\mathbf{Q}(\sqrt[3]{2})$ *no es extensión de Galois de* $\mathbf{Q}$.

b) Encontrar una extensión de Galois de $\mathbf{Q}$ *que contiene a* $\mathbf{Q}(\sqrt[3]{2})$ *como subcuerpo.*

$\equiv$

a) $\sqrt[3]{2}$ tiene a $x^3-2 \in \mathbf{Q}[x]$ como polinomio mínimo sobre $\mathbf{Q}$. Entonces $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$. Si $\mathbf{Q}(\sqrt[3]{2})$ fuese extensión de Galois de $\mathbf{Q}$, se tendría que $o(G(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q})) = 3$, pero ésto no es así ya que seguidamente demostramos que $G(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}) = \{1_{\mathbf{Q}(\sqrt[3]{2})}\}$: Sea φ un automorfismo de $\mathbf{Q}(\sqrt[3]{2})$ que fija $\mathbf{Q}$. Entonces, como $\varphi(\sqrt[3]{2})$ ha de ser raíz de x^3-2, ha de pertenecer a $\mathbf{Q}(\sqrt[3]{2})$ y observando que

$$x^3-2 \;=\; x^3-(\sqrt[3]{2})^3 \;=\; (x-\sqrt[3]{2})(x^2+\sqrt[3]{2}\cdot x+\sqrt[3]{4})$$

sólo tiene a $\sqrt[3]{2}$ como raíz en $\mathbf{Q}(\sqrt[3]{2})$, , tenemos que $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$, lo que implica que $\varphi = 1_{\mathbf{Q}(\sqrt[3]{2})}$.

b) Sea E el cuerpo raíz en $\mathbf{C}$ del polinomio x^3-2. En un ejercicio anteriormente resuelto vimos que, llamando $\alpha := \sqrt[3]{2}$, $\beta := \frac{\sqrt[3]{2}}{2}(-1+i\sqrt{3})$, se tiene que $E = \mathbf{Q}(\alpha, \beta)$ y que $[E : \mathbf{Q}] = 6$. También all se demostró que $G(E/\mathbf{Q}) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6\}$, donde esos automorfismos se pueden identificar con las permutaciones del conjunto de las raíces de x^3-2, que es $U := \{\alpha, \beta, \overline{\beta}\}$. Así

$$\varphi_1 \equiv Id_U, \quad \varphi_2 \equiv (\beta, \overline{\beta}), \quad \varphi_3 \equiv (\alpha, \beta), \quad \varphi_4 \equiv (\alpha, \beta, \overline{\beta}), \quad \varphi_5 \equiv (\alpha, \overline{\beta}), \quad \varphi_6 \equiv (\alpha, \overline{\beta}, \beta).$$

Aplicando el teorema de Artin, ya que $[E : \mathbf{Q}] = 6 = o(G(E/F))$, se tiene que $E = \mathbf{Q}(\alpha, \beta)$ es una extensión de Galois de $\mathbf{Q}$ que contiene a $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt[3]{2})$. $\clubsuit$

Ex. 241 *Sea* $E = F(\alpha)$ *una extensión de Galois de* F. *Si* $Gal(E/F) = \{\Phi_1, \Phi_2, ..., \Phi_n\}$, *demostrar que*

$$[x-\Phi_1(\alpha)][x-\Phi_2(\alpha)]...[x-\Phi_n(\alpha)]$$

es un polinomio mínimo de α *sobre* F.

$\equiv$

Como $E = F(\alpha)$ es extensión de Galois de F, sabemos que $[E : F] = o(Gal(E/F)) = n$. Si llamamos

$$f(x) \ := \ [x - \Phi_1(\alpha)][x - \Phi_2(\alpha)]...[x - \Phi_n(\alpha)],$$

suponiendo que $\Phi_1 = 1_E$, está claro que $f(\alpha) = 0$. Puesto que todo polinomio mínimo de α sobre F tiene por grado $[F(\alpha) : F] = n$, para poder afirmar que $f(x)$ es polinomio mínimo de α sobre F sólo nos hace falta ver que $f(x) \in F[x]$. Para ello, desarrollando

$$f(x) \ = \ x^n - [\Phi_1(\alpha) + \Phi_2(\alpha) + ... + \Phi_2(\alpha)]x^{n-1} + [\Phi_1(\alpha)\Phi_2(\alpha) + ... + \Phi_{n-1}(\alpha)\Phi_n(\alpha)]x^{n-2}$$

$$+... + (-1)^n\Phi_1(\alpha)\Phi_2(\alpha)...\Phi_n(\alpha).$$

Fijando, para cada $k = 1, 2, ..., n$

$$c_k \ = \ (-1)^k \sum_{1\leq j_1<j_1<...<j_k\leq n} \Phi_{j_1}(\alpha)\Phi_{j_2}(\alpha)...\Phi_{j_k}(\alpha)$$

tenemos que

$$f(x) \ = \ x^n \ + \ c_1x^{n-1} \ + \ c_2x^{n-2} \ + \ ... \ + \ c_n.$$

Así pues todo consiste en demostrar que $c_k \in F, \ 1 \leq k \leq n$. Pero, como F es el cuerpo fijo de los automorfismos Φ_h, $1 \leq h \leq n$, basta con ver que, para cada $h, k \in \{1, 2, ..., n\}$, $\Phi_h(c_k) = c_k$.

$$\Phi_h(c_k) \ = \ \Phi_h[(-1)^k \sum_{1\leq j_1<j_1<...<j_k\leq n} \Phi_{j_1}(\alpha)\Phi_{j_2}(\alpha)...\Phi_{j_k}(\alpha)]$$

$$= (-1)^k \sum_{1\leq j_1<j_1<...<j_k\leq n} \Phi_h[\Phi_{j_1}(\alpha)]\Phi_h[\Phi_{j_2}(\alpha)]...\Phi_h[\Phi_{j_k}(\alpha)]$$

$$= (-1)^k \sum_{1\leq j_1<j_1<...<j_k\leq n} (\Phi_h\Phi_{j_1})(\alpha)(\Phi_h\Phi_{j_2})(\alpha)...(\Phi_h\Phi_{j_k})(\alpha) = (*)$$

Pero, al ser elementos de un grupo de aplicaciones

$$\{ \ \Phi_h\Phi_{j_1}, \Phi_h\Phi_{j_2}, ..., \Phi_h\Phi_{j_k}\} \ = \ \{\Phi_{r_1}, \Phi_{r_2}, ..., \Phi_{r_k}\}.$$

Por tanto, siguiendo de lo anterior

$$(*) \ = \ (-1)^k \sum_{1\leq 1<r_1<...<r_k\leq n} \Phi_{r_1}(\alpha)\Phi_{r_2}(\alpha)...\Phi_{r_k}(\alpha) \ = \ c_k. \ \clubsuit$$

Ex. 242 *Sea E una extensión de Galois de F. Sea $\alpha \in E$ un elemento tal que ningún automorfismo de E, salvo la identidad, lo deja fijo. Demostrar que $E = F(\alpha)$.*

$\equiv$

Supongamos que $[E : F] = o(Gal(E/F)) = n$. Entonces podemos escribir $Gal(E/F) = \{\Phi_1, \Phi_2, ..., \Phi_n\}$, con $\Phi_1 = 1_E$. Consideremos el polinomio

$$f(x) \ := \ [x - \Phi_1(\alpha)][x - \Phi_2(\alpha)]...[x - \Phi_n(\alpha)].$$

Del ejercicio anterior, sabemos que $f(x) \in F[x]$. Veamos que $f(x)$ es polinomio mínimo de α sobre F. Para empezar, $f(\alpha) = 0$. Además, si $1 \leq i \neq j \leq n$, se tiene que $\Phi_i(\alpha) \neq \Phi_j(\alpha)$, ya que, de lo contrario

$$\Phi_i(\alpha) = \Phi_j(\alpha) \rightarrow (\Phi_i\Phi_j^{-1})(\alpha) = \alpha \overset{(hipòtesis)}{\rightarrow} \Phi_i\Phi_j^{-1} = 1_E \rightarrow \Phi_i = \Phi_j. \text{ Absurdo}$$

Por otra parte, para $i = 1, 2, ..., n$, tenemos que $\Phi_i(\alpha) \notin F$, de lo contrario

$$\exists c \in F \text{ tal que } \Phi_i(\alpha) = c \rightarrow \Phi_i(c) \overset{(c \in F)}{=} c = \Phi_i(\alpha) \overset{(\Phi_i \ biyect.)}{\rightarrow} c = \alpha. \text{ Absurdo, pues } \alpha \notin F.$$

Por lo tanto, $f(x)$ es un polinomio irreducible sobre F y se trata de un polinomio mínimo de α sobre F. Consecuentemente

$$\left.\begin{array}{l} [F(\alpha) : F] = grado(f(x)) = n \\ [E : F] = n \\ F(\alpha) \subset E \end{array}\right\} \Rightarrow E = F(\alpha). \clubsuit$$

Ex. 243 *Sea E una extensión de $\mathbf{Z}_p$ (p primo, evidentemente) tal que $[E : \mathbf{Z}_p] = n$. Dado que E^* es un grupo cíclico multiplicativo, sabemos que, si θ es el generador de E^*, se tiene que $E = \mathbf{Z}_p(\theta)$. Sea* $\begin{array}{rccc} \Phi & : & E & \longrightarrow & E \\ & & \alpha & \rightarrow & \Phi(\alpha) := \alpha^p \end{array}$ *. Demostrar*

a) $\{1_E, \Phi, \Phi^2, ..., \Phi^{n-1}\}$ es un grupo de automorfismos de E que fijan $\mathbf{Z}_p$.

b) E es una extensión de Galois de F cuyo grupo de Galois es el grupo de automorfismos anterior.

≡

Antes de meternos con los dos apartados del ejercicio, veamos que en efecto $E = \mathbf{Z}_p(\theta)$. Es evidente que $E \supset \mathbf{Z}_p(\theta)$. Recíprocamente, si $\alpha \in E$, suponemos que $\alpha \neq 0$ ($\alpha = 0 \in \mathbf{Z}_p(\alpha)$, por definición de $\mathbf{Z}_p(\alpha)$); entonces $\alpha \in E^*$ implica que existe $m \in \mathbf{N}$ tal que $\alpha = \theta^m \in \mathbf{Z}_p(\theta)$.

a) Para $k = 1, 2, ..., n-1$, veamos que Φ^k es un automorfismo de E. Para ello, como la composición de automorfismos lo sigue siendo, todo se reduce a ver que Φ lo es. Así, dados $\alpha, \beta \in E$, puesto que $carac(\mathbf{Z}_p) = p$,

$$\Phi(\alpha + \beta) = (\alpha + \beta)^p = \alpha^p + \beta^p = \Phi(\alpha) + \Phi(\beta)$$

$$\Phi(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \Phi(\alpha)\Phi(\beta).$$

Si $\alpha \in Ker(\Phi$, entonces

$$0 = \Phi(\alpha) = \alpha^p \rightarrow \alpha = 0.$$

Por tanto, al ser Φ una aplicación inyectiva de un conjunto finito ($E = \mathbf{Z}_p(\theta)$ tiene p^n elementos, ya que $E \cong \mathbf{Z}_p^n$) en sí mismo, se deduce que Φ es una biyección.

Para ver que Φ^k, $1 \leq k \leq n-1$, fija $\mathbf{Z}_p$, basta con ver que lo hace Φ. Así

$$\alpha \in E^*,\ \alpha = \Phi(\alpha) = \alpha^p \leftrightarrow 0 = \alpha^p - \alpha = \alpha(\alpha^{p-1} - 1) \leftrightarrow \alpha^{p-1} - 1 = 0 \leftrightarrow \alpha^{p-1} = 1.$$

Acabamos de ver que, en $(E^*, \cdot)$, el orden de α es menor o igual que $p-1$, pero éso caracteriza a los elementos de $\mathbf{Z}_p^*$, i.e., $\alpha \in \mathbf{Z}_p^*$. Finalmente, veamos que $\{1_E, \Phi, \Phi^2, ..., \Phi^{n-1}\}$ es un grupo. Para ello basta con comprobar que $\Phi^n = 1_E$, lo cual es evidente: Dado $\alpha \in E$

$$\Phi^n(\alpha) \;=\; \alpha^{p^n} \;=\; \alpha \cdot \alpha^{p^n-1} \;=\; \alpha,$$

ya que $o(\alpha) \mid o(\theta) = p^n - 1$.

b) En virtud del teorema de Artin, puesto que $[E : \mathbf{Z}_p] = n = o(\{1_E, \Phi, ..., \Phi^{n-1}\})$, sólo tenemos que probar que dichos automorfismos de E son los únicos que fijan $\mathbf{Z}_p$. Así, sea φ un automorfismo de E fijando $\mathbf{Z}_p$. Como $E = \mathbf{Z}_p(\theta)$ y $[E : \mathbf{Z}_p] = n$, existe un polinomio mínimo de θ sobre $\mathbf{Z}_p$ de grado n. Sea $f(x) = c_0 + c_1x + ... + c_nx^n \in \mathbf{Z}_p[x]$ dicho polinomio. Entonces $\varphi(\theta)$ también es una raíz de $f(x)$. Pero, veamos que $\theta^p, \theta^{p^2}, ..., \theta^{p^{n-1}}$ también son raíces de $f(x)$

$$\begin{aligned}
&c_0 + c_1\theta^p + c_2\theta^{2p} + ... + c_n\theta^{np} = (c_0 + c_1\theta + c_2\theta^2 + ... + c_n\theta^n)^p = 0\\
&c_0 + c_1\theta^{p^2} + c_2\theta^{2p^2} + ... + c_n\theta^{np^2} = (c_0 + c_1\theta + c_2\theta^2 + ... + c_n\theta^n)^{p^2} = 0\\
&.....\\
&.....\\
&c_0 + c_1\theta^{p^{n-1}} + c_2\theta^{2p^{n-1}} + ... + c_n\theta^{np^{n-1}} = (c_0 + c_1\theta + c_2\theta^2 + ... + c_n\theta^n)^{p^{n-1}} = 0.
\end{aligned}$$

Por tanto, $\varphi(\theta) \in \{\theta, \theta^p, ..., \theta^{p^{n-1}}\}$ y entonces

$$\begin{aligned}
&\varphi(\theta) = \theta \;\rightarrow\; \varphi = 1_E\\
&\varphi(\theta) = \theta^p \;\rightarrow\; \varphi = \Phi\\
&.....\\
&.....\\
&\varphi(\theta) = \theta^{p^{n-1}} \;\rightarrow\; \varphi = \Phi^{n-1}.
\end{aligned}$$

Así pues E es una extensión de Galois de $\mathbf{Z}_p$ tal que $Gal(E/\mathbf{Z}_p) = \{1_E, \Phi, \Phi^2, ..., \Phi^{n-1}\}$. ♣

Ex. 244 *Dar un ejemplo de una extensión finita separable pero no normal.*

≡

Aunque ya lo hemos definido con anterioridad, lo volvemos a repetir: Una extensión E de F es una extensión normal siempre que cualquier polinomio de $F[x]$ irreducible sobre F que admite alguna raíz en E se descompone totalmente en E. Consideremos $E := \mathbf{Q}(\sqrt[3]{2})$. Como $x^3 - 2$ es polinomio mínimo de $\sqrt[3]{2}$ sobre $\mathbf{Q}$, deducimos que $[E : \mathbf{Q}] = 3$, por lo que E es una extensión finita de $\mathbf{Q}$. Al ser $carac(E) = carac(\mathbf{Q}) = 0$, por definición, E es separable. Para ver que E no es una extensión normal de $\mathbf{Q}$, observemos que $x^3 - 2$ posee una raíz en E (que es $\sqrt[3]{2}$), pero no se descompone totalmente en E, ya que

$$x^3 - 2 \;=\; (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}),$$

donde $x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$ no tiene raíces en E, pues

$$x^2+\sqrt[3]{2}x+\sqrt[3]{4} = 0 \rightarrow x = \frac{-\sqrt[3]{2} \pm \sqrt{\sqrt[3]{4} - 4\sqrt[3]{4}}}{2} = \frac{-\sqrt[3]{2} \pm \sqrt{-3\sqrt[3]{4}}}{2} = \frac{-\sqrt[3]{2} \pm \mathbf{i}\sqrt[3]{2}\sqrt{3}}{2} \notin E.\clubsuit$$

Ex. 245 *Dar un ejemplo de extensión separable normal que no sea finita.*

≡

Consideremos el cuerpo complejo $\mathbf{C}$. Claramente, $\mathbf{C}$ es una extensión no algebraica (trascendente) de $\mathbf{Q}$, por lo que no es extensión finita de $\mathbf{Q}$. Como $carac(\mathbf{C}) = 0$, se trata de una extensión separable. Finalmente, del Teorema Fundamental del Algebra, sabemos que todo polinomio de $\mathbf{Q}[x]$ se descompone toalmente en $\mathbf{C}$, por tanto $\mathbf{C}$ es una extensión normal de $\mathbf{Q}$. ♣

Nota 23 Notar que, aunque el cuerpo real $\mathbf{R}$ es una etensión trascendente separable de $\mathbf{Q}$, no sirve como respuesta del ejercicio previo ya que $\mathbf{R}$ no es un cuerpo algebraicamente cerrado ($\mathbf{C}$ sí lo es), por lo que $\mathbf{R}$ no es extensión normal de $\mathbf{Q}$.

Ex. 246 *Consideremos los cuerpos $E = \mathbf{Z}_p(x)$ y $F = \mathbf{Z}_p(x^p)$, i.e., los cuerpos de las fracciones polinómicas de coeficientes en $\mathbf{Z}_p$ (p primo) de variable x y de variable x^p, respectivamente. Demostrar que E es una extensión finita normal no separable de F.*

≡

Sabemos (o debemos saber) que E y F son sendos cuerpos. Además, $F \subset E$, pues toda fracción polinómica en x^p lo es en x. Veamos que se trata de una extensión finita, en concreto demostramos que $\{1, x, x^2, ..., x^{p-1}\}$ es un sistema generador de E sobre F (de hecho es una base).

Sea $\frac{f(x)}{g(x)} \in E$. Suponiendo que $g(x) = c_0 + c_1x + ... + c_nx^n \in \mathbf{Z}_p[x]$, observemos que

$$g(x)^p = (c_0 + c_1x + ... + c_nx^n)^p \overset{(carac(\mathbf{Z}_p)=p)}{=} c_0^p + c_1^p x^p + ... + c_n^p (x^p)^n$$

$$\overset{(o(\mathbf{Z}_p^*)=p-1)}{=} c_0 + c_1x^p + ... + c_n(x^p)^n = g(x^p).$$

Entonces

$$\frac{f(x)}{g(x)} = \frac{f(x)g(x)^{p-1}}{g(x)^p} = \frac{f(x)g(x)^{p-1}}{g(x^p)} = \frac{1}{g(x^p)}[f(x)g(x)^{p-1}].$$

Llamemos $h(x) := f(x)g(x)^{p-1}$. Como $\frac{1}{g(x^p)} \in F$, para tener que $\frac{f(x)}{g(x)}$ está generado por $\{1, x, x^2, ..., x^{p-1}\}$ basta con ver que $h(x)$ está generado por dicho conjunto. Supongamos que $h(x) = a_0 + a_1x + ... + a_mx^m$. Entonces, dividiendo m por p, sea $m = pq + r$,

$$h(x) = a_0 + a_1x + ... + a_mx^m = a_0 + a_1x + ... + a_{p-1}x^{p-1} + a_px^p + a_{p+1}x^px + ... + a_m(x^p)^qx^r$$

$$= (a_0 + a_px^p) + (a_1 + a_{p+1}x^p)x + ... + (a_r + a_mx^{pq})x^r + a_{r+1}x^{r+1} + ... + a_{p-1}x^{p-1}.$$

Claramente, como $a_0 + a_px^p, a_1 + a_{p+1}x^p, ..., a_r + a_mx^{pq} \in F$, tenemos que $h(x)$ es una combinación lineal sobre F de $\{1, x, x^2, ..., x^{p-1}\}$. Por tanto, puesto que no es difícil comprobar que $\{1, x, x^2, ..., x^{p-1}\}$ es un conjunto de vectores linealmente independientes sobre F, se tiene que $[E : F] = p$.

Seguidamente veamos que E es una extensión normal de F. Sea $\widehat{f}(y) \in F[y]$ un polinomio irreducible sobre F tal que admite una raíz $\alpha \in E$. De lo visto antes, sabemos que $\alpha^p \in F$. Así, considerando el polinomio

$$\widehat{g}(y) := y^p - \alpha^p \in F[y], \qquad \widehat{g}(\alpha) = 0,$$

tenemos que, ya que $\widehat{f}(y)$ es un polinomio mínimo de α sobre F, $\widehat{f}(y)$ es un divisor de $\widehat{g}(y)$, es decir

$$\widehat{f}(y) \mid \widehat{g}(y) = y^p - \alpha^p = (y-\alpha)^p.$$

Ello implica que $\widehat{f}(y)$ es una potencia del binomio $y - \alpha$, luego $\widehat{f}(y)$ se descompone totalmente en E.

Finalmente, lo que acabamos de ver nos dice que E no es extensión separable de F, ya que el polinomio $\widehat{g}(y) = y^p - \alpha^p \in F[x]$, con $\alpha \in E \setminus F$, es un polinomio irreducible sobre F tal que, como $p \geq 2$, y, $\widehat{g}(y) = (x-\alpha)^p$, no se descompone en factores distintos. ♣

Ex. 247 *Demostrar que si E es una extensión de Galois de F, entonces sólo existe un número finito de cuerpos entre E y F.*

≡

Antes recordemos lo que dice el Teorema Fundamental de la Teoría de Galois (*TFTG*): *Sea E una extensión de Galois de F. Entonces existe una correspondencia biunívoca entre los cuerpos intermedios entr F y E (llamados subextensiones de E/F) y los subgrupos de $Gal(E/F)$. Explícitamente*

1) Si K es una subextensión de E/F, entonces le corresponde el subgrupo $G(E/K)$, i.e., el grupo de los automorfismos de E que fijan K, y se cumple

$$[K:F] = [Gal(E/F) : G(E/K)] = \frac{o(Gal(E/F))}{o(G(E/K))}.$$

Es más, si $Gal(E/F)$ es un grupo normal, entonces, de la igualdad anterior, $[K:F] = o(G(K/F))$ y se deduce que K es extensión de Galois de F.

2) Si H es un subgrupo de $Gal(E/F)$, entonces le corresponde el subcuerpo de E que fija H, i.e., el cuerpo fijo de H, que representamos como F_H.

Si $F \subset K \subset E$, del Teorema Fundamental de la Teoría de Galois, E es una extensión de K y su grupo de automorfismos que fijan K, $G(E/K)$, es un subgrupo de $Gal(E/F)$. Como $Gal(E/F)$ es un grupo finito, sólo admite una cantidad finita de subgrupos. Así pues, para demostrar lo que nos pide el enunciado, todo se reduce a ver que, si K_1 y K_2 son cuerpos contenidos entre F y E tales que $G(E/K_1) = G(E/K_2)$, entonces $K_1 = K_2$. Para ello, representando mediante F_φ al cuerpo fijo del automorfismo φ,

$$K_1 = \bigcap_{\varphi \in G(E/K_1)} F_\varphi = \bigcap_{\varphi \in G(E/K_2)} F_\varphi = K_2. \clubsuit$$

Ex. 248 *Sean* $\zeta = e^{\frac{2\pi i}{7}}$ *y* $E = \mathbf{Q}(\zeta)$.

a) Demostrar que E *es extensión de Galois de* $\mathbf{Q}$ *y determinar* $Gal(E/\mathbf{Q})$.

b) Hallar todos los cuerpos entre $\mathbf{Q}$ *y* E, *con el subgrupo de* $Gal(E/\mathbf{Q})$ *correspondiente, indicando cuáles de ellos son extensiones de Galois de* $\mathbf{Q}$.

$\equiv$

a) Como ζ es una raíz séptima compleja de la unidad y

$$x^7 - 1 \;=\; (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1),$$

se tiene que $f(x) := x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbf{Q}[x]$ es un polinomio mínimo de ζ sobre $\mathbf{Q}$, por lo que $[E : \mathbf{Q}] = 6$. Es inmediato comprobar que las raíces de $f(x)$ forman el conjunto

$$U_7 \;=\; \{\, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6 \,\},$$

de donde, como para un automorfismo Φ de E que fije $\mathbf{Q}$, se tiene que $\Phi(\zeta) \in U_7$, deducimos que los distintos elementos del grupo de los automorfismos de E que fijan$\mathbf{Q}$, $G(E/\mathbf{Q})$, son

$$G(E/\mathbf{Q}) \;=\; \{\, \Phi_1, \Phi_2, \Phi_3, \Phi_4, \Phi_5, \Phi_6 \,\},$$

de modo que, para $k = 1, 2, 3, 4, 5, 6$, $\Phi_k(\zeta) = \zeta^k$. Haciendo uso del teorema de Artin, como $o(G(E/\mathbf{Q})) = 6 = [E : \mathbf{Q}]$, tenemos que E es extensión de Galois de $\mathbf{Q}$ y $Gal(E/\mathbf{Q}) = G(E/F) = \{\, \Phi_1, \Phi_2, \Phi_3, \Phi_4, \Phi_5, \Phi_6 \,\}$.

b) La Tabla de Cayley del grupo $Gal(E/\mathbf{Q})$ es

$\circ$	Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6
Φ_1	Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6
Φ_2	Φ_2	Φ_4	Φ_6	Φ_1	Φ_3	Φ_5
Φ_3	Φ_3	Φ_6	Φ_2	Φ_5	Φ_1	Φ_4
Φ_4	Φ_4	Φ_1	Φ_5	Φ_2	Φ_6	Φ_3
Φ_5	Φ_5	Φ_3	Φ_1	Φ_6	Φ_4	Φ_2
Φ_6	Φ_6	Φ_5	Φ_4	Φ_3	Φ_2	Φ_1 .

Empleando notación del grupo simétrico de un conjunto de 6 elementos

$$\Phi_1 \equiv Id,\; \Phi_2 \equiv (124)(365),\; \Phi_3 \equiv (132645),$$

$$\Phi_4 \equiv (142)(356),\; \Phi_5 \equiv (154623),\; \Phi_6 \equiv (16)(25)(34).$$

Por tanto, los únicos subgrupos propios de $Gal(E/\mathbf{Q})$ son $H_1 := \{\Phi_1, \Phi_6\}$ y $H_2 := \{\Phi_1, \Phi_2, \Phi_4\}$. Sean K_1 y K_2 los cuerpos fijos de H_1 y H_2, respectivamente. Claramente, $\mathbf{Q} \subset K_1$ y $\mathbf{Q} \subset K_2$. Vamos a calcular dichos cuerpos.

Si $\alpha = c_0 + c_1\zeta + c_2\zeta^2 + c_3\zeta^3 + c_4\zeta^4 + c_5\zeta^5 \in K_1 = F_{\Phi_6}$, entonces

$$\alpha = \Phi_6(\alpha) \rightarrow\; c_0 + c_1\zeta + c_2\zeta^2 + c_3\zeta^3 + c_4\zeta^4 + c_5\zeta^5 = c_0 + c_1\zeta^6 + c_2\zeta^5 + c_3\zeta^4 + c_4\zeta^3 + c_5\zeta^2$$

de lo que, como $\zeta^6 = -1 - \zeta - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5$,

$$\left.\begin{array}{l} c_0 - c_1 = c_0 \rightarrow\ c_1 = 0 \\ c_2 = c_5 \\ c_3 = c_4 \end{array}\right\} \rightarrow\ \alpha = c_0 + c_2(\zeta^2 + \zeta^5) + c_3(\zeta^3 + \zeta^4),$$

de donde

$$K_1 \ = \ [1, \zeta^2 + \zeta^5, \zeta^3 + \zeta^4]_{\mathbf{Q}} \ \Rightarrow\ [K_1 : \mathbf{Q}] = 3.$$

Análogamente, si $\alpha = c_0 + c_1\zeta + c_2\zeta^2 + c_3\zeta^3 + c_4\zeta^4 + c_5\zeta^5 \in K_2 = F_{\Phi_2} \cap F_{\Phi_4}$, entonces

$$\alpha = \Phi_2(\alpha) = \Phi_4(\alpha) \rightarrow \left\{\begin{array}{l} c_3 = c_5 = 0 \\ c_1 = c_2 = c_4 \end{array}\right\} \rightarrow\ \alpha = c_0 + c_1(\zeta + \zeta^2 + \zeta^4),$$

de donde

$$K_2 \ = \ [1, \zeta + \zeta^2 + \zeta^4]_{\mathbf{Q}} \ \Rightarrow\ [K_2 : \mathbf{Q}] = 2.$$

Del $TFTG$, como $Gal(E/\mathbf{Q}) = \langle\ \Phi_3\ \rangle$ es cíclico y, por tanto, normal, se tiene que

$$\begin{array}{rcl} o(G(K_1/\mathbf{Q})) & = & [Gal(E/\mathbf{Q}) : G(E/K_1] \ = \ [K_1 : \mathbf{Q}] \\ o(G(K_2/\mathbf{Q})) & = & [Gal(E/\mathbf{Q}) : G(E/K_2] \ = \ [K_2 : \mathbf{Q}], \end{array}$$

por lo que K_1 y K_2 son extensiones de Galois de $\mathbf{Q}$. Los grupos de Galois correspondientes son H_1 y H_2. ♣

Nota 24 Aunque el ejercicio anterior ya está resuelto, en aras de una mejor comprensión, veamos que $K_1 = \mathbf{Q}(\zeta + \zeta^6)$: Como $K_1 = [1, \zeta^2 + \zeta^5, \zeta^3 + \zeta^4]_{\mathbf{Q}}$, y puesto que $\zeta + \zeta^6 = -1 - (\zeta^2 + \zeta^5) - (\zeta^3 + \zeta^4)$, está claro que $\mathbf{Q} \subset \mathbf{Q}(\zeta + \zeta^6) \subset K_1$. Además, del $TFTG$, existe un subgrupo H tal que $H = G(E/\mathbf{Q}(\zeta + \zeta^6))$. Pero, como el orden de inclusión de las torres de cuerpos es inverso al de sus grupos, tenemos $H_1 \subset H \subset Gal(E/\mathbf{Q})$, lo que implica que $o(H)$ es un divisor propio par (pues $o(H_1) = 2 \mid o(H)$) de 6. Claramente, $o(H) = 2 = o(H_1)$, de lo que $H = H_1$ y entonces $K_1 = \mathbf{Q}(\zeta + \zeta^6)$.

De manera análoga se demuestra que $K_2 = \mathbf{Q}(\zeta + \zeta^2 + \zeta^4)$: Es evidente que $\mathbf{Q} \subset \mathbf{Q}(\zeta + \zeta^2 + \zeta^4) \subset K_2$, por lo que, del $TFTG$, existe un subgrupo H' tal que $H' = G(E/\mathbf{Q}(\zeta + \zeta^2 + \zeta^4))$. Entonces $H_2 \subset H' \subset Gal(E/\mathbf{Q})$ implica que $o(H')$ es un divisor propio de 6 mayor o igual que 3. Consecuentemente, $H' = H_2$ y $\mathbf{Q}(\zeta + \zeta^2 + \zeta^4) = K_2$.

Ex. 249 *Sea E una extensión de Galois de F. Sean K_1 y K_2 dos cuerpos intermedios entre F y E. Se dice que K_1 y K_2 son conjugados siempre que existe un automorfismo $\Phi \in Gal(E/F)$ tal que $\Phi(K_1) = K_2$. Demostrar que K_1 y K_2 son conjugados si y sólo si $G(E/K_1)$ y $G(E/K_2)$ son subgrupos conjugados de $Gal(E/F)$.*

$\equiv$

[$\Rightarrow$] Supongamos que K_1 y K_2 son cuerpos intermedios entre F y E conjugados. Por definición, existe un automorfismo $\Phi \in Gal(E/F)$ tal que $\Phi(K_1) = K_2$. Para ver que $G(E/K_1)$ y $G(E/K_2)$ son subgrupos conjugados de $Gal(E/F)$ todo se reduce a demostrar

que $\Phi\ G(E/K_1)\ \Phi^{-1} = G(E/K_2)$: Si $\varphi \in \Phi\ G(E/K_1)\ \Phi^{-1}$, existe $\psi \in G(E/K_1)$ tal que $\varphi = \Phi\psi\Phi^{-1}$. Como $\Phi(K_1) = K_2$, dado $\beta \in K_2$, existe $\alpha \in K_1$ tal que $\Phi(\alpha) = \beta$. Así

$$\varphi(\beta) = \Phi\psi\Phi^{-1}(\beta) = \Phi\psi(\alpha) \overset{(\psi \in G(E/K_1))}{=} \Phi(\alpha) = \beta.$$

Por tanto, $\varphi \in G(E/K_2)$. Recíprocamente, sea $\varphi \in G(E/K_2)$. Definimos $\psi := \Phi^{-1}\varphi\Phi$. Claramente, $\psi \in Gal(E/F)$; veamos que $\psi \in G(E/K_1)$: Dado $\alpha \in K_1$

$$\psi(\alpha) = \Phi^{-1}\varphi\Phi(\alpha) \overset{(\varphi \in G(E/K_2))}{=} \Phi^{-1}\Phi(\alpha) = \alpha.$$

Entonces $\varphi = \Phi\psi\Phi^{-1} \in \Phi\ G(E/K_1)\ \Phi^{-1}$.
[$\Leftarrow$] Suponiendo ahora que $G(E/K_1)$ y $G(E/K_2)$ son subgrupos conjugados de $Gal(E/F)$, por definición de subgrupos conjugados, existe $\Phi \in Gal(E/F)$ tal que $\Phi\ G(E/K_1)\ \Phi^{-1} = G(E/K_2)$. Para terminar, veamos que $\Phi(K_1) = K_2$: Dado $\alpha \in K_1$

$$\forall \varphi \in G(E/K_2) = \Phi\ G(E/K_1)\ \Phi^{-1},\ \ \Phi^{-1}\varphi\Phi \in G(E/K_1)$$

$$\rightarrow\ \alpha = \Phi^{-1}\varphi\Phi(\alpha)\ \rightarrow\ \Phi(\alpha) = \varphi[\Phi(\alpha)].$$

Esto implica que $\Phi(\alpha)$ pertenece al cuerpo fijo de $G(E/K_2)$, i.e., $\Phi(\alpha) \in K_2$. Hemos probado pues que $\Phi(K_1) \subset K_2$. Recíprocamente, sea $\beta \in K_2$. Como antes

$$\forall \varphi \in G(E/K_1) = \Phi^{-1}\ G(E/K_2)\ \Phi,\ \ \Phi\varphi\Phi^{-1} \in G(E/K_2)\ \rightarrow\ \beta = \Phi\varphi\Phi^{-1}(\beta)$$

Por tanto, $\Phi^{-1}(\beta) = \varphi[\Phi^{-1}(\beta)]$. Al ser cierto para cualquier elemento de $G(E/K_1)$, podemos afirmar que $\Phi^{-1}(\beta) \in K_1$, es decir, $\beta \in \Phi(K_1)$. ♣

Ex. 250 *Sea E una extensión de Galois de F tal que $Gal(E/F)$ es un grupo cíclico de orden n. Demostrar que se cumplen las siguientes afirmaciones*

a) Si $d \mid n$, entonces existe un único cuerpo intermedio K tal que $[E : K] = d$.

b) Si K_1 y K_2 son cuerpos intermedios, entonces

$$K_1 \subset K_2 \quad \text{si y sólo si} \quad [E : K_2] \mid [E : K_1].$$

≡

a) Sea $Gal(E/F) = \{Id, \Phi, \Phi^2, ..., \Phi^{n-1}\}$. Consideremos el subgrupo

$$H := \langle\ \Phi^{\frac{n}{d}}\ \rangle = \{\ Id, \Phi^{\frac{n}{d}}, \Phi^{\frac{2n}{d}}, ..., \Phi^{\frac{(d-1)n}{d}}\ \}.$$

Entonces H es un subgrupo de $Gal(E/F)$ de orden d. Sea K el cuerpo fijo de H en E. Claramente, E es una extensión de Galois de K (notar que, al ser $Gal(E/F)$ cíclico, es normal y entonces E es extensión de Galois de todo cuerpo intermedio) tal que $[E : K] = o(Gal(E/K)) = o(H) = d$. Para demostrar la unicidad de K, supongamos que D es un cuerpo intermedio entre F y E tal que $[E : D] = d$. Entonces, como E es extensión de Galois de D, se tiene que $d = [E : D] = o(G(E/D))$. Así, como $Gal(E/D) \subset Gal(E/F)$, existe un $k \in \{1, 2, ..., n-1\}$ de modo que $Gal(E/D) = \langle\ \Phi^k\ \rangle$, con $o(\Phi^k) = d$. Pero

$$d = o(\Phi^k) = \frac{n}{mcd(k,n)} \rightarrow mcd(k,n) = \frac{n}{d} \rightarrow \frac{n}{d} \mid k$$

$$\rightarrow \exists m \in \mathbf{N} \ / \ k = m\frac{n}{d} \rightarrow \ \Phi^k = (\Phi^{\frac{n}{d}})^m \in H.$$

Así, $Gal(E/D) \subset H$ y entonces $Gal(E/D)$ y H son dos grupos del mismo orden encadenados. Por tanto, $Gal(E/D) = H = Gal(E/K)$, de donde $D = K$.

b) Sean $F \subset K_1, K_2 \subset E$.

[$\Rightarrow$] Supongamos que $K_1 \subset K_2$. Entonces $F \subset K_1 \subset K_2 \subset E$. Al tratarse de subgrupos de un grupo cíclico, normal por tanto, cada cuerpo es extensión de Galois de cualquier subcuerpo. Así

$$K_2 \text{ es ext. de Galois de } K_1 \ \Rightarrow \ Gal(K_2/K_1) \cong Gal(E/K_1)/Gal(E/K_2)$$

$$\Rightarrow \ [K_2 : K_1] = o(Gal(K_2/K_1)) = \frac{o(Gal(E/K_1))}{o(Gal(E/K_2))} = \frac{[E : K_1]}{[E : K_2]}.$$

Luego $[E : K_2]$ divide a $[E : K_1]$.

[$\Leftarrow$] Supongamos ahora que $[E : K_2]$ divide a $[E : K_1]$. Al ser extensiones de Galois todas

$$\left.\begin{array}{l} [E : K_1] = o(Gal(E/K_1)) \\ [E : K_2] = o(Gal(E/K_2)) \end{array}\right\} \ \Rightarrow \ o(Gal(E/K_2)) \mid o(Gal(E/K_1)).$$

Llamando $d_1 := o(Gal(E/K_1))$, $d_2 := o(Gal(E/K_2))$ y aplicando la resolución del apartado a) de este ejercicio, podemos afirmar que K_1 es el único cuerpo intermedio tal que es el cuerpo fijo de $Gal(E/K_1) = \langle \ \Phi^{\frac{n}{d_1}} \ \rangle$ y, similarmente, K_2 es el único cuerpo intermedio tal que es el cuerpo fijode $Gal(E/K_2) = \langle \ \Phi^{\frac{n}{d_2}} \ \rangle$. Ahora bien

$$\frac{\frac{n}{d_2}}{\frac{n}{d_1}} = \frac{d_1}{d_2} \rightarrow \frac{n}{d_1} \mid \frac{n}{d_2},$$

ello implica que $\Phi^{\frac{n}{d_2}} \in Gal(E/K_1)$, de donde $Gal(E/K_2) \subset Gal(E/K_1)$. Como ya sabemos (orden de las torres inverso al orden de los grupos fijos), tenemos que $K_1 \subset K_2$ (de toda formas, para verlo directamente, cójase un elemento arbitrario de K_1 y un automorfismo arbitrario de $Gal(E/K_2)$; como el automorfismo también pertenece a $Gal(E/K_1)$, el automorfismo fija al elemento. Por tanto, el elemento pertenece al cuerpo fijo de $Gal(E/K_2)$, o sea, a K_2). ♣

Ex. 251 *[Recíproco del ejercicio previo]*

Demostrar que si una extensión de Galois E de F cumple las condiciones a) y b) del ejercicio anterior, entonces $Gal(E/F)$ es cíclico.

≡

Sea $o(Gal(E/F)) = p_1^{m_1}p_2^{m_2}...p_k^{m_k}$, donde $p_1, p_2, ..., p_k$ son primos distintos. Aplicando la condición a) del ejercicio anterior, para cada $i = 1, 2, ..., k$, existe un único cuerpo intermedio K_i entre F y E tal que $[E : K_i] = p_i^{m_i}$. Consecuentemente, podemos afirmar que $G(E/K_i)$ es el único subgrupo p_i-Sylow de $Gal(E/F)$. De un problema resuelto en la parte de Teoría de Grupos, sabemos que

$$Gal(E/F) \ = \ G(E/K_1)G(E/K_2)...G(E/K_k).$$

De otro problema correspondiente a la parte de grupos, sabemos que, al ser $Gal(E/F)$ un producto directo de una cantidad finita de grupos con órdenes primos entre sí, si probamos que cada factor $G(E/K_i)$, $1 \leq i \leq k$, es cíclico, podemos afirmar que $Gal(E/F)$ también lo es. Así pues, veamos que $G(E/K_i)$ es un grupo cíclico. De nuevo utilizando resultados demostrados en la parte de grupos, para tener que $G(E/K_i)$ es cíclico basta con ver que, si H_1 y H_2 son subgrupos de $G(E/K_i)$, entonces, o bien $H_1 \subset H_2$, o bien $H_2 \subset H_1$. Del $TFTG$, existen cuerpos intermedios D_1 y D_2 entre F y E tales que $H_1 = G(E/D_1)$ y $H_2 = G(E/D_2)$. Como $o(G(E/D_1))$ y $o(G(E/D_2))$ son divisores de $p_i^{m_i}$, tenemos que $o(G(E/D_1)) \mid o(G(E/D_2))$, ó al revés $o(G(E/D_2)) \mid o(G(E/D_1))$. Supongamos que $o(G(E/D_1)) \mid o(G(E/D_2))$. Entonces, como $[E : D_1] = o(G(E/D_1))$ y $[E : D_2] = o(G(E/D_2))$, se tiene que $[E : D_1] \mid [E : D_2]$. La condición b) garantiza que $D_2 \subset D_1$, de donde

$$H_1 = G(E/D_1) \subset G(E/D_2) = H_2. \clubsuit$$

Ex. 252 *Sea E una extensión finita de F y sean K_1, K_2 cuerpos intermedios tales que ningún subcuerpo propio de E contiene a $K_1 \cup K_2$. Demostrar*

1) *Si K_1 es extensión de Galois de F, entonces E es extensión de Galois de K_2, siendo $Gal(E/K_2)$ isomorfo a un subgrupo de $Gal(K_1/F)$.*
2) *Bajo las condiciones del apartado anterior, si $K_1 \cap K_2 = F$, entonces $Gal(E/K_2) \cong Gal(K_1/F)$.*

$\equiv$

1) Suponiendo que K_1 es extensión de Galois de F, del $TFTG$ sabemos que, como $F \subset K_1 \cap K_2 \subset K_1$, K_1 es una exrtensión de Galois de $K_1 \cap K_2$. Llamando H_2 al grupo de los automorfismos de E que fijan K_2, veamos para empezar que H_2 es isomorfo a $Gal(K_1/K_1 \cap K_2)$. Para ello, definimos

$$\begin{array}{rccc} f & : & H_2 & \longrightarrow & Gal(K_1/K_1 \cap K_2) \\ & & \Phi & \to & f(\Phi) := \Phi_{|K_1}. \end{array}$$

f bien definida: Claramente, si $\Phi \in H_2$, $f(\Phi) \in \mathcal{G}(K_1)$. Además, dado $\alpha \in K_1 \cap K_2$

$$f(\Phi)(\alpha) = \Phi_{|K_1}(\alpha) \overset{(\alpha \in K_1)}{=} \Phi(\alpha) \overset{(\alpha \in K_2)}{=} \alpha,$$

por lo que $f(\Phi) \in Gal(K_1/K_1 \cap K_2)$.
f homomorfismo de grupos: Dados $\Phi_1, \Phi_2 \in H_2$

$$f(\Phi_1 \circ \Phi_2) = (\Phi_1 \circ \Phi_2)_{|K_1} = (\Phi_1)_{|K_1} \circ (\Phi_2)_{|K_1} = f(\Phi_1) \circ f(\Phi_2).$$

f inyectivo: Si $\Phi \in Ker(f)$, entonces

$$\left.\begin{array}{l} \Phi \in H_2 \\ Id_{K_1} = f(\Phi) = \Phi_{|K_1} \end{array}\right\} \Rightarrow \Phi \text{ fija a } K_1 \cup K_2.$$

Como el cuerpo fijo de Φ es un subcuerpo de E que contiene a $K_1 \cup K_2$, de la hipótesis de partida, podemos afirmar que Φ fija a todo E, es decir, $\Phi = Id_E$.
f sobre: Si $\varphi \in Gal(K_1/K_1 \cap K_2)$, al ser E el único subcuerpo que contiene a $K_1 \cup K_2$, queda claro que E coincide con el cuerpo formado por todos los elementos de la forma

$$\frac{\sum_{i=1}^{n} \alpha_{i1}\alpha_{i2}}{\sum_{j=1}^{m} \beta_{j1}\beta_{j2}}, \quad \alpha_{i1}, \beta_{j1} \in K_1,\ \alpha_{i2}, \beta_{j2} \in K_2,\ 1 \le i \le n,\ 1 \le j \le m.$$

Así, definimos

$$\begin{array}{rcl} \Phi : E & \longrightarrow & E \\ \frac{\sum_{i=1}^{n} \alpha_{i1}\alpha_{i2}}{\sum_{j=1}^{m} \beta_{j1}\beta_{j2}} & \to & \Phi(\frac{\sum_{i=1}^{n} \alpha_{i1}\alpha_{i2}}{\sum_{j=1}^{m} \beta_{j1}\beta_{j2}}) := \frac{\sum_{i=1}^{n} \varphi(\alpha_{i1})\alpha_{i2}}{\sum_{j=1}^{m} \varphi(\beta_{j1})\beta_{j2}}. \end{array}$$

Es directo comprobar (aunque un poco rollo...) que $\Phi \in \mathcal{G}(E)$. Además, si $\alpha_2 \in K_2$, de la definición de Φ tenemos que $\Phi(\alpha_2) = \alpha_2$, es decir, $\Phi \in H_2$. Finalmente, dado $\alpha_1 \in K_1$, otra vez de la definición de Φ

$$\Phi(\alpha_1) = \varphi(\alpha_1) \Rightarrow \varphi = \Phi_{|K_1} = f(\Phi).$$

Denotando por F_{H_2} al cuerpo fijo del grupo H_2, obviamente $K_2 \subset F_{H_2}$. Además, si $\alpha \in K_1 \cap F_{H_2}$, se tiene que

$$\forall \varphi \in Gal(K_1/K_1 \cap K_2), \quad \varphi(\alpha) \overset{(\Phi := f^{-1}(\varphi))}{=} f(\Phi)(\alpha) = \Phi_{|K_1}(\alpha) = \alpha,$$

lo que implica que α pertenece al cuerpo fijo del grupo $Gal(K_1/K_1 \cap K_2)$ que es $K_1 \cap K_2$. Hemos demostrado por tanto que $K_1 \cap F_{H_2} = K_1 \cap K_2$. Así, la situación es la siguiente, reprentamos por K_1K_2 al menor subcuerpo conteniendo $K_1 \cup K_2$,

$$\left.\begin{array}{l} K_2 \subset F_{H_2} \\ K_1 \cap F_{H_2} = K_1 \cap K_2 \\ K_1K_2 = K_1F_{H_2} = E \end{array}\right\} \Rightarrow K_2 = F_{H_2} \Rightarrow \left\{\begin{array}{l} E \text{ es ext. de Galois de } K_2 \\ Gal(E/K_2) = H_2 \\ \cong Gal(K_1/K_1 \cap K_2) \subset Gal(K_1/F). \end{array}\right.$$

2) Si $K_1 \cap K_2 = F$, entonces, de lo visto antes,

$$Gal(E/K_2) = H_2 \cong Gal(K_1/K_1 \cap K_2) = Gal(K_1/F). \ \clubsuit$$

Ex. 253 *Con las mismas hipótesis del ejercicio anterior, demostrar que si K_1 y K_2 son extensiones de Galois de F, entonces*

1) E es extensión de Galois de F, y
2) $Gal(E/F) \cong Gal(E/K_1) \times Gal(E/K_2)$, si $K_1 \cap K_2 = F$.

$\equiv$
1) Suponiendo que K_1 y K_2 son extensiones de Galois de F, sabemos del ejercicio previo que E es extensión de Galois tanto de K_1 como de K_2. Sea H el grupo de los automorfismos de E que fijan F y sea F_H el cuerpo fijo de H. Veamos que $F = F_H$:
$[\subset]$ Evidente, pues, $\forall \varphi \in H$, $F \subset F_\varphi$.

[$\supset$] Si $\alpha \in F_H$, entonces, dado $\Phi \in Gal(E/K_1) \subset H$, se tiene que $\alpha = \Phi(\alpha)$, por lo que $\alpha \in K_1$, al ser K_1 el cuerpo fijo de $Gal(E/K_1)$. Además, dado $\varphi \in Gal(K_1/F)$, de la resolución del ejercicio anterior, sabemos que existe $\Phi \in \mathcal{G}(E)$ tal que $\varphi = \Phi_{|K_1}$. Así

$$\Phi_{|F} = \varphi_{|F} = Id_F \overset{(\Phi \text{ fija } F)}{\to} \Phi \in H \to \alpha = \Phi(\alpha) \overset{(\alpha \in K_1)}{=} \varphi(\alpha).$$

Ello implica que, $\forall \varphi \in Gal(K_1/F)$, $\varphi(\alpha) = \alpha$, de donde $\alpha \in F$.

Por tanto, $F = F_H$ y, como $o(H) \leq [E : F] < \infty$, deducimos que E es extensión de Galois de F.

2) Definimos

$$\begin{array}{ccc} f : Gal(E/F) & \longrightarrow & Gal(K_1/F) \times Gal(K_2/F) \\ \Phi & \to & f(\Phi) := (\Phi_{|K_1}, \Phi_{|K_2}). \end{array}$$

Es evidente que la aplicación f está bien definida.

f homomorfismo de grupos: También es evidente.

f inyectivo: Si $\Phi \in Ker(f)$, entonces

$$(Id_{K_1}, Id_{K_2}) = f(\Phi) = (\Phi_{|K_1}, \Phi_{|K_2}) \Rightarrow \left\{ \begin{array}{c} \Phi \text{ fija } K_1 \\ \Phi \text{ fija } K_2 \end{array} \right\} \Rightarrow \Phi \text{ fija } K_1 \cup K_2.$$

Como E es el único cuerpo que contiene a $K_1 \cup K_2$, se tiene que Φ fija E,ie., $\Phi = Id_E$.

Así pues, hemos demostrado que $Gal(E/F)$ es isomorfo a un subgrupo de $Gal(K_1/F) \times Gal(K_2/F)$. Como $F = K_1 \cap K_2$, de lo hecho en el ejercicio previo

$$\begin{array}{l} Gal(E/K_1) \cong Gal(K_2/F) \\ Gal(E/K_2) \cong Gal(K_1/F). \end{array}$$

Ello implica que $Gal(E/F)$ es isomorfo a un subgrupo de $Gal(E/K_1) \times Gal(E/K_2)$. Pero

$$o(Gal(E/F)) = [E : F] = [E : K_1][K_1 : F]$$

$$= o(Gal(E/K_1))o(Gal(K_1/F)) = o(Gal(E/K_1))o(Gal(E/K_2)),$$

de donde se deduce que $Gal(E/F) \cong Gal(E/K_1) \times Gal(E/K_2)$. ♣

Ex. 254 *Sea* $\mathbf{C}(x)$ *el cuerpo de las fracciones racionales sobre* $\mathbf{C}$. *Consideremos las seis aplicaciones* $\Phi_i : \mathbf{C}(x) \to \mathbf{C}(x)$, $1 \leq i \leq 6$, *dadas por*

$$\Phi_1[f(x)] = f(x); \quad \Phi_2[f(x)] = f(1-x); \quad \Phi_3[f(x)] = f(\frac{1}{x}); \quad \Phi_4[f(x)] = f(\frac{x-1}{x});$$

$$\Phi_5[f(x)] = f(\frac{1}{1-x}); \quad \Phi_1[f(x)] = f(\frac{x}{x-1}).$$

Demostrar que

a) $G = \{\Phi_1, \Phi_2, \Phi_3, \Phi_4, \Phi_5, \Phi_6\}$ *es un grupo de automorfismos de* $\mathbf{C}(x)$.

b) Determinar el cuerpo fijo de G.

c) Hallar todos los cuerpos intermedios que existen entre F_G *y* $\mathbf{C}(x)$.

$\equiv$

a) Es evidente que $\Phi_1 \in \mathcal{G}(\mathbf{C}(x))$, ya que se trata de la identidad de $\mathbf{C}(x)$. Demostramos que $\Phi \in \mathcal{G}(\mathbf{C}(x))$, las demás aplicaciones se ve que son autoorfismos de manera simlar.
Φ_2 homomorfismo de cuerpos: Sean $f(x), g(x) \in \mathbf{C}(x)$

$$\Phi_2[f(x)+g(x)] = f(1-x)+g(1-x) = \Phi_2[f(x)]+\Phi_2[g(x)]$$
$$\Phi_2[f(x)g(x)] = f(1-x)g(1-x) = \Phi_2[f(x)]\Phi_2[g(x)].$$

Φ_2 inyectivo: Si $f(x) \in Ker(\Phi_2)$, entonces

$$0 \;=\; \Phi_2[f(x)] \;=\; f(1-x) \;\;\Rightarrow\;\; f(x) \;=\; 0.$$

Φ_2 sobre: Si $g(x) \in \mathbf{C}(x)$, entonces buscamos $f(x) \in \mathbf{C}(x)$ tal que

$$g(x) \;=\; \Phi_2[f(x)] \;=\; f(1-x) \overset{(cambio:\ t=1-x \to x=1-t)}{\Rightarrow} f(x) \;:=\; g(1-x) \in \mathbf{C}(x).$$

Para ver que el conjunto G arriba descrito es un subgrupo de $\mathcal{G}(\mathbf{C}(x))$, basta con mirar su tabla de Cayley

$\circ$	Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6
Φ_1	Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6
Φ_2	Φ_2	Φ_1	Φ_4	Φ_3	Φ_6	Φ_5
Φ_3	Φ_3	Φ_5	Φ_1	Φ_6	Φ_2	Φ_4
Φ_4	Φ_4	Φ_6	Φ_2	Φ_5	Φ_1	Φ_3
Φ_5	Φ_5	Φ_3	Φ_6	Φ_1	Φ_4	Φ_2
Φ_6	Φ_6	Φ_4	Φ_5	Φ_2	Φ_3	Φ_1 .

b) Como habitualmente hacemos, representamos por F_G al cuerpo fijo del grupo G. Veamos que

$$F_G \;=\; F_{\Phi_2} \cap F_{\Phi_3} \;=\; \{\; f(x) \in \mathbf{C}(x) \;:\; f(x) = f(1-x) = f(\frac{1}{x}) \;\}.$$

[$\subset$] Evidente, ya que $F_G = F_{\Phi_1} \cap F_{\Phi_2} \cap F_{\Phi_3} \cap F_{\Phi_4} \cap F_{\Phi_5} \cap F_{\Phi_6}$.
[$\supset$] Sea $f(x) \in F_{\Phi_2} \cap F_{\Phi_3}$. Entonces

$$\left.\begin{array}{l} \Phi_4[f(x)] = \Phi_2[\Phi_3[f(x)]] = \Phi_2[f(x)] = f(x) \to\ f(x) \in F_{\Phi_4} \\ \Phi_5[f(x)] = \Phi_3[\Phi_2[f(x)]] = \Phi_3[f(x)] = f(x) \to\ f(x) \in F_{\Phi_5} \\ \Phi_6[f(x)] = \Phi_2[\Phi_5[f(x)]] = \Phi_2[f(x)] = f(x) \to\ f(x) \in F_{\Phi_6} \end{array}\right\} \;\Rightarrow\; f(x) \in F_G.$$

c) Veamos que los únicos subcuerpos entre F_G y $\mathbf{C}(x)$ son

$$F_{\Phi_2};\quad F_{\Phi_3};\quad F_{\Phi_6};\quad F_{\Phi_4} \cap F_{\Phi_5}.$$

Sea K un cuerpo intermedio entre F_G y $\mathbf{C}(x)$. Por el $TFTG$, $\mathbf{C}(x)$ es una extensión de Galois de K. Por tanto, $Gal(\mathbf{C}(x)/K)$ es un subgrupo de $Gal(\mathbf{C}(x)/F_G) = G$. Así, todo

consiste en buscar subgrupos del grupo G de arriba. Explícitamente, $Gal(\mathbf{C}(x)/K)$ ha de ser uno de los cuatro subgrupos propios que tiene G, es decir

$$Gal(\mathbf{C}(x)/K) \in \{\ H_1 := \{\Phi_1, \Phi_2\},\ H_2 := \{\Phi_1, \Phi_3\},\ H_3 := \{\Phi_1, \Phi_6\},\ H_4 := \{\Phi_1, \Phi_4, \Phi_5\}\}.$$

Consecuentemente, K ha de coincidir con alguno de los cuerpos fijos de estos subgrupos. Así

$$\begin{aligned} F_{H_1} &= F_{\Phi_2} \\ F_{H_2} &= F_{\Phi_3} \\ F_{H_3} &= F_{\Phi_6} \\ F_{H_4} &= F_{\Phi_4} \cap F_{\Phi_5}. \clubsuit \end{aligned}$$

Nota 25 Como se ha podido apreciar en la resolución del ejercicio previo, uno de los grandes éxitos del Teorema Fundamental de la Teoría de Galois reside en el hecho de que, si se quieren encontrar cuerpos intermedios entre un cuerpo dado y una extensión de Galois suya, basta con buscar subgrupos de un grupo finito, lo que usualmente es mucho más fácil y cómodo.

Ex. 255 *Demostrar que toda extensión finita de un cuerpo finito es de Galois y su grupo de Galois es cíclico*

≡

Sea F un cuerpo finito tal que $card(F) = p^n$, con $carac(F) = p$. Sea E una extensión finita de F con $[E : F] = m$. Al ser E isomorfo a F^m (como espacio vectorial sobre F), tenemos que $card(E) = p^{mn}$. Del teorema de Artin, para demostrar que E es extensión de Galois de F, todo se reduce a hallar un grupo de m automorfismos de E que fijen F. Así, definimos

$$\begin{aligned} \varphi\ :\ E &\longrightarrow E \\ \alpha &\to \varphi(\alpha) := \alpha^p. \end{aligned}$$

Como ya hemos hecho en anteriores ejercicios, es bastante fácil verificar que $\varphi \in \mathcal{G}(E)$. Consideremos el conjunto

$$H\ :=\ \{Id_E, \varphi^n, \varphi^{2n}, ..., \varphi^{(m-1)n}\ \}.$$

Claramente $H \subset \mathcal{G}(E)$. Veamos que se trata de automorfismos distintos: Todo se reduce a ver que, para $i = 1, 2, ...m-1$, $\varphi^{ni} \neq Id_E$. De lo contrario, para $\alpha \in E$

$$\alpha\ =\ \varphi^{ni}(\alpha)\ =\ \alpha^{p^{ni}}\ \to\ 1\ =\ \alpha^{p^{ni}-1}.$$

Ello contradice el que E^* es un grupo multiplicativo cíclico de orden $p^{nm}-1$. Además, para $i = 1, 2, ...m-1$, el automorfismo φ^{in} fija F, ya que, si $a \in F$, entonces

$$\varphi^n(\alpha)\ =\ \alpha^{p^n}\ = \alpha \cdot \alpha^{p^n-1} \overset{(F^* \text{ grupo multiplicativo de orden } p^n-1)}{=} \alpha,$$

de donde $\varphi^{in}(\alpha) = (\varphi^n \circ \overset{(i)}{\ldots} \circ \varphi^n)(\alpha) = \alpha$. Hemos terminado de resolver este ejercicio puesto que, del teorema de Artin, E es una extensión de Galois de F cuyo grupo de Galois es $Gal(E/F) = H = \langle\ \varphi^n\ \rangle$, ya que $(\varphi^n)^m = Id_E$. $\clubsuit$

Nota 26 Puede demostrarse sin mucha dificultad que

$$\mathcal{G}(E) \;=\; \langle\, \varphi \,\rangle \;=\; \{\, Id_E, \varphi, \varphi^2, ..., \varphi^{mn-1} \,\},$$

de lo que

$$o(\varphi^n) \;=\; \frac{o(\varphi)}{mcd(o(\varphi), n)} \;=\; \frac{mn}{n} \;=\; m,$$

como ya sabíamos.

Ex. 256 *Determinar el grupo de Galois $Gal(E/F)$, siendo E el cuerpo raíz del polinomio $f(x) = x^6 - 8$, en los siguientes casos*

a) $F = \mathbf{Q}$, *b)* $F = \mathbf{Q}(\sqrt{2})$, *c)* $F = \mathbf{Q}(\omega)$, $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{3}}$.

$\equiv$

Del teorema de Artin, al ser E cuerpo raíz del polinomio

$$f(x) \;=\; x^6 - 8 \;=\; (x - \sqrt{2})(x - \sqrt{2}\mathrm{e}^{\frac{2\pi \mathrm{i}}{6}})(x - \sqrt{2}\mathrm{e}^{\frac{2\cdot 2\pi \mathrm{i}}{6}})...(x - \sqrt{2}\mathrm{e}^{\frac{5\cdot 2\pi \mathrm{i}}{6}}),$$

se tiene que E es una extensión de Galois de cualquier cuerpo intermedio entre $\mathbf{Q}$ y E. Por tanto, E es extensión de Galois de F en cualquiera de los tres casos planteados, por lo que tiene sentido preguntarnos por $Gal(E/F)$.

a) Llamando por comodidad: $\alpha := \sqrt{2}$, $\beta := \mathrm{e}^{\frac{2\pi \mathrm{i}}{6}}$, tenemos que

$$f(x) \;=\; x^6 - 8 \;=\; (x - \alpha)(x - \alpha\beta)(x - \alpha\beta^2)...(x - \alpha\beta^5).$$

Entonces, está claro que

$$E \;=\; \mathbf{Q}(\alpha, \alpha\beta, \alpha\beta^2, ..., \alpha\beta^5) \;=\; \mathbf{Q}(\alpha, \beta).$$

Como ahora $F = \mathbf{Q}$, tenemos que hallar $Gal(E/\mathbf{Q})$. Así, si $\Phi \in Gal(E/\mathbf{Q})$, como Φ transforma raíces de $f(x)$ en raíces del mismo polinomio

$$\left.\begin{array}{l} \exists i \in \{0,1,2,3,4,5\}/\Phi(\alpha) = \alpha\beta^i \\ \exists j \in \{0,1,2,3,4,5\}/\Phi(\alpha\beta) = \alpha\beta^j \end{array}\right\}$$

$$\Rightarrow \alpha\beta^j = \Phi(\alpha\beta) = \Phi(\alpha)\Phi(\beta) = \alpha\beta^i\Phi(\beta) \Rightarrow\; \Phi(\beta) = \beta^{j-i}.$$

Eso nos dice que $\Phi(\beta) \in \langle\, \beta \,\rangle$. Pero, como $\Phi_{|\langle\, \beta \,\rangle}$ es un isomorfismo del grupo multiplicativo $\langle\, \beta \,\rangle$ en sí mismo, deducimos que $\Phi(\beta) \in \{\beta, \beta^5\}$, ya que β y β^5 son los únicos elementos de dicho grupo de orden $6 = o(\beta)$. Como Φ queda determinado por sus imágenes de α y de β, tenemos que

$$Gal(E/\mathbf{Q}) \;=\; \{\, \Phi_{ij} \;:\; 0 \le i \le 5,\; j \in \{1,5\} \,\}, \quad \text{siendo} \quad \begin{array}{rcl} \Phi_{ij}: E & \to & E \\ \alpha & \to & \alpha\beta^i \\ \beta & \to & \beta^j. \end{array}$$

Por tanto, aunque no nos lo pregunten,

$$[E:\mathbf{Q}] \;=\; o(Gal(E/\mathbf{Q})) \;=\; 12.$$

b) Aquí $F = \mathbf{Q}(\alpha)$, con la misma notación del apartado previo. Claramente, $E = \mathbf{Q}(\alpha,\beta) = F(\beta)$. Si $\Phi \in Gal(E/F)$, como vimos antes que $\Phi(\beta) \in \{\beta, \beta^5\}$, se tiene que

$$Gal(E/F) \;=\; \{\, Id_E = \Phi_{01},\ \Phi_{05}\,\}.$$

Así

$$[E:\mathbf{Q}(\sqrt{2})] \;=\; o(Gal(E/\mathbf{Q}(\sqrt{2}))) \;=\; 2.$$

Notar que, como $E = \mathbf{Q}(\sqrt{2})(\beta) = \{z = a + b\beta \;:\; a,b \in \mathbf{Q}(\sqrt{2})\}$, podemos explicitar

$$\begin{array}{rcl} \Phi_{05} & : & E \longrightarrow E \\ & & z = a + b\beta \;\to\; \overline{z} = a + b\overline{\beta}, \end{array}$$

ya que

$$\Phi_{05}(a+b\beta) = a + b\Phi_{05}(\beta) = a + b\beta^5 = a + b\mathrm{e}^{\frac{10\pi\mathbf{i}}{6}} = a + b\mathrm{e}^{\frac{12\pi\mathbf{i}-2\pi\mathbf{i}}{6}} = a + b\mathrm{e}^{\frac{-2\pi\mathbf{i}}{6}} = a + b\overline{\beta}.$$

c) En este apartado, usando la notación fijada desde el principio, $F = \mathbf{Q}(\omega)$, con $\omega = \mathrm{e}^{\frac{2\pi\mathbf{i}}{3}} = \beta^2 = \frac{-1+\mathbf{i}\sqrt{3}}{2}$. Observemos que

$$\omega \;-\; \beta \;=\; \frac{-1+\mathbf{i}\sqrt{3}}{2} \;-\; (\cos\frac{\pi}{3} + \mathbf{i}\sin\frac{\pi}{3}) \;=\; -1,$$

de donde $\omega = -1 + \beta \in \mathbf{Q}(\beta)$ y $F = \mathbf{Q}(\omega) = \mathbf{Q}(\beta)$. Por lo tanto, $E = \mathbf{Q}(\alpha,\beta) = \mathbf{Q}(\beta)(\alpha) = F(\alpha)$. Si $\Phi \in Gal(E/F) = Gal(E/\mathbf{Q}(\beta))$, entonces, de lo visto antes, puesto que, al tener que fijar $F = \mathbf{Q}(\beta)$, $\Phi(\beta) = \beta$,

$$\exists i \in \{0,1,2,3,4,5\} \;/\; \Phi(\alpha) = \alpha\beta^i \;\Rightarrow\; \Phi \in \{\Phi_{01}, \Phi_{11}, \Phi_{21}, \Phi_{31}, \Phi_{41}, \Phi_{51},\}.$$

Es decir

$$Gal(E/\mathbf{Q}(\omega)) \;=\; \{\Phi_{01}, \Phi_{11}, \Phi_{21}, \Phi_{31}, \Phi_{41}, \Phi_{51},\}.$$

Consecuentemente

$$[E:\mathbf{Q}(\omega)] \;=\; o(Gal(E/\mathbf{Q}(\omega)) \;=\; 6. \;\clubsuit$$

Ex. 257 *Analizar de forma completa la extensión de Galois* $E = \mathbf{Q}(\zeta)$, $\zeta = \mathrm{e}^{\frac{2\pi\mathbf{i}}{7}}$, *determinando todos los cuerpos intermedios, sean o no extensiones de Galois de* $\mathbf{Q}$, *así como todos los grupos de Galois que aparecen.*

≡

Como $E = \mathbf{Q}(\zeta)$, todo automorfismo $\varphi \in Gal(E/\mathbf{Q})$ es tá determinado por el valor $\varphi(\zeta)$. Por lo tanto

$$Gal(E/\mathbf{Q}) \;=\; \{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6\,\}, \quad \text{siendo } \varphi_i(\zeta) = \zeta^i,\ 1 \le i \le 6.$$

Si K es un cuerpo intermedio, es decir, $\mathbf{Q} \subset K \subset E$, entonces el grupo de automorfismos de E que fijan K, $G(E/K)$, es un subgrupo de $Gal(E/\mathbf{Q})$. Pero este grupo de Galois es cíclico, ya que $Gal(E/\mathbf{Q}) = \langle\ \varphi_3\ \rangle$, por ello todo subgrupo suyo es normal y $G(E/K)$ es normal en $Gal(E/\mathbf{Q})$. Del $TFTG$, sabemos que K es extensión de Galois de $\mathbf{Q}$ y que $Gal(K/\mathbf{Q}) = Gal(E/\mathbf{Q})/Gal(E/K)$. Ahora determinemos todos los subgrupos propios de $Gal(E/\mathbf{Q})$ para poder tener todos los posibles cuerpos intermedios.

$$H_1 := \langle\ \varphi_1\ \rangle = \{\varphi_1, \varphi_6\}; \quad H_2 := \langle\ \varphi_2\ \rangle = \{\varphi_1, \varphi_2, \varphi_4\}.$$

Sean K_1 y K_2 los cuerpos fijos de H_1 y de H_2, respectivamente. Entonces

$$\left.\begin{array}{l} \sum_{j=0}^{6} a_j\zeta^j \in K_1 \ \leftrightarrow\ \varphi_6(\sum_{j=0}^{6} a_j\zeta^j) = \sum_{j=0}^{6} a_j\zeta^j \\ \sum_{j=0}^{6} a_j\zeta^j \in K_2 \ \leftrightarrow\ \varphi_2(\sum_{j=0}^{6} a_j\zeta^j) = \sum_{j=0}^{6} a_j\zeta^j \end{array}\right\}$$

$$\Rightarrow \left\{\begin{array}{l} K_1 = \{a_0 + a_1(\zeta + \zeta^6) + a_2(\zeta^2 + \zeta^5) + a_3(\zeta^3 + \zeta^4) :\ a_0, a_1, a_2, a_3 \in \mathbf{Q}\} \\ K_2 = \{a_0 + a_1(\zeta + \zeta^2 + \zeta^4) + a_3(\zeta^3 + \zeta^5 + \zeta^6) :\ a_0, a_1, a_3 \in \mathbf{Q}\}. \end{array}\right.$$

Por tanto

$$\left\{\begin{array}{lllll} [K_1 : \mathbf{Q}] & = & \frac{[E:\mathbf{Q}]}{[E:K_1]} & = & \frac{6}{o(Gal(E/K_1))} = \frac{6}{o(H_1)} = \frac{6}{2} = 3 \\ [K_2 : \mathbf{Q}] & = & \frac{[E:\mathbf{Q}]}{[E:K_2]} & = & \frac{6}{o(Gal(E/K_2))} = \frac{6}{o(H_2)} = \frac{6}{2} = 3. \end{array}\right.$$

Es más

$$0 = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6$$

$$\rightarrow \left\{\begin{array}{l} \zeta^3 + \zeta^4 \in \mathbf{Q}(\zeta, \zeta^6, \zeta^2 + \zeta^5) \\ (\zeta + \zeta^6)(\zeta^2 + \zeta^5) = \zeta + \zeta^3 + \zeta^4 + \zeta^6 \rightarrow\ \zeta + \zeta^6 \in \mathbf{Q}(\zeta^2 + \zeta^5) \end{array}\right\},$$

de donde $K_1 = \mathbf{Q}(\zeta^2 + \zeta^5) = \mathbf{Q}(\sin\frac{3\pi}{7})$, pues

$$\zeta^2 + \zeta^5 = 1_{\frac{4\pi}{7}} + 1_{\frac{10\pi}{7}} = \cos\frac{4\pi}{7} + \cos\frac{10\pi}{7} + \mathbf{i}(\sin\frac{4\pi}{7} + \sin\frac{10\pi}{7})$$

$$= 2\cos\pi\sin\frac{3\pi}{7} + \mathbf{i}\cdot 2\sin\pi\sin\frac{3\pi}{7} = -2\sin\frac{3\pi}{7}.$$

Similarmente se vé que

$$K_2 = \mathbf{Q}(\zeta + \zeta^2 + \zeta^4).$$

Notar que

$$K_1 \cap K_2 = \mathbf{Q}, \quad K_1K_2 = E,$$

pues

$$\begin{array}{lllll} Gal(E/K_1 \cap K_2) & \supset & Gal(E/K_1)\cdot Gal(E/K_2) & = & H_1H_2 = Gal(E/\mathbf{Q}) \\ Gal(E/K_1 \cap K_2) & \subset & Gal(E/K_1) \cap Gal(E/K_2) & = & H_1 \cap H_2 = \{\varphi_1 = Id_E\}. \clubsuit \end{array}$$

3.3. Polinomios simétricos

Ex. 258 *Expresar mediante las funciones simétricas elementales los siguientes polinomios simétricos*

a) $f(x_1,x_2,x_3) = x_1^2+x_2^2+x_3^2+x_1x_2+x_2x_3+x_1x_3$.
b) $g(x_1,x_2,x_3) = x_1^2x_2^2+x_2^2x_3^2+x_1^2x_3^2$.
c) $h(x_1,x_2,x_3) = x_1^3+x_2^3+x_3^3$.
d) $p(x_1,x_2,x_3) = x_1^4+x_2^4+x_3^4$.
e) $q(x_1,x_2,x_3) = (x_1-x_2)^2(x_2-x_3)^2(x_1-x_3)^2$.

$\equiv$

Recordemos que, para tres variables x_1,x_2,x_3, las funciones simétricas elementales son

$$\begin{aligned}\sigma_1 &= x_1+x_2+x_3\\ \sigma_2 &= x_1x_2+x_2x_3+x_1x_3\\ \sigma_3 &= x_1x_2x_3.\end{aligned}$$

a)

$$\sigma_1^2-\sigma_2 = (x_1+x_2+x_3)^2-(x_1x_2+x_2x_3+x_1x_3)$$

$$= x_1^2+x_2^2+x_3^2+2x_1x_2+2x_2x_3+2x_1x_3-(x_1x_2+x_2x_3+x_1x_3).$$

Por tanto, $f(x_1,x_2,x_3) = \sigma_1^2-\sigma_2$.
b)

$$\sigma_2^2-2\sigma_1\sigma_3 = (x_1x_2+x_2x_3+x_1x_3)^2-2(x_1+x_2+x_3)(x_1x_2x_3)$$

$$= x_1^2x_2^2+x_1^2x_3^2+x_2^2x_3^2+2x_1^2x_2x_3+2x_1x_2^2x_3+2x_1x_2x_3^2-2x_1^2x_2x_3-2x_1x_2^2x_3-2x_1x_2x_3^2$$

$$= x_1^2x_2^2+x_2^2x_3^2+x_1^2x_3^2.$$

Luego $g(x_1,x_2,x_3) = \sigma_2^2-2\sigma_1\sigma_3$.
c)

$$(x_1+x_2+x_3)^3-3(x_1+x_2+x_3)(x_1x_2+x_2x_3+x_1x_3)+3x_1x_2x_3$$

$$= x_1^3+x_2^3+x_3^3+3(x_1^2x_2+x_1^2x_3+x_1x_2^2+x_2^2x_3+x_1x_3^2+x_2x_3^2)+6x_1x_2x_3$$

$$-3(x_1^2x_2+x_1^2x_3+x_1x_2^2+x_2^2x_3+x_1x_3^2+x_2x_3^2+3x_1x_2x_3)+3x_1x_2x_3 = x_1^3+x_2^3+x_3^3.$$

Así, $h(x_1,x_2,x_3) = \sigma_1^3-3\sigma_1\sigma_2+3\sigma_3$.
d) Veamos que $p(x_1,x_2,x_3) = \sigma_1^4-4\sigma_1^2\sigma_2+2\sigma_2^2+4\sigma_1\sigma_3$.

$$\sigma_1^4-4\sigma_1^2\sigma_2+2\sigma_2^2+4\sigma_1\sigma_3 = (\sigma_1^2-2\sigma_2)^2-2\sigma_2^2+4\sigma_1\sigma_3$$

$$\overset{(b)}{=} (x_1^2+x_2^2+x_3^2)^2-2g(x_1,x_2,x_3)$$

$$= x_1^4+x_2^4+x_3^4+2(x_1^2x_2^2+x_1^2x_x^2+x_2^2x_3^2)-2(x_1^2x_2^2+x_1^2x_x^2+x_2^2x_3^2) = x_1^4+x_2^4+x_3^4.$$

e) Observemos inicialmente que $(x_1 - x_2)(x_2 - x_3)(x_1 - x_3)$ equivale al valor del determinante de Vardermonde de orden 3 dado por

$$\begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{vmatrix}.$$

Por tanto

$$q(x_1,x_2,x_3) = \begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{vmatrix}^2 = det[\begin{pmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{pmatrix} \cdot \begin{pmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{pmatrix}]$$

$$= \begin{vmatrix} 3 & x_1+x_2+x_3 & x_1^2+x_2^2+x_3^2 \\ x_1+x_2+x_3 & x_1^2+x_2^2+x_3^2 & x_1^3+x_2^3+x_3^3 \\ x_1^2+x_2^2+x_3^2 & x_1^3+x_2^3+x_3^3 & x_1^4+x_2^4+x_3^4 \end{vmatrix}$$

$$\overset{(a:=x_1^2+x_2^2+x_3^2)}{=} \begin{vmatrix} 3 & \sigma_1 & a \\ \sigma_1 & a & h(x_1,x_2,x_3) \\ a & h(x_1,x_2,x_3) & p(x_1,x_2,x_3) \end{vmatrix}$$

$$\overset{(h=h(x_1,x_2,x_3),\ p=p(x_1,x_2,x_3))}{=} 3ap + 2\sigma_1 ha - a^3 - \sigma_1^2 p - 3h^2$$

$$= 3(\sigma_1^2 - 2\sigma_2)(\sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3) + 2\sigma_1((\sigma_1^2 - 2\sigma_2)(\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3) - (\sigma_1^2 - 2\sigma_2)^3$$

$$-\sigma_1^2(\sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3) - 3(\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3^2) = \sigma_1^2\sigma_2^2 - 4\sigma_1^3\sigma_3 - 4\sigma_2^3 + 18\sigma_1\sigma_2\sigma_3 - 27\sigma_3^2. \clubsuit$$

Nota 27 La expresión del polinomio simétrico $q(x_1, x_2, x_3)$ del ejercicio anterior puede encontrarse en [2, pág. 188].

Ex. 259 *Sea, para cada* $k \in \mathbf{N}$, $\pi_k(x_1, x_2, ..., x_n) = x_1^k + x_2^k + ... + x_n^k$. *Demostrar las siguientes igualdades*

$$\left.\begin{array}{l} 1)\ \text{Si } k \leq n, \quad \pi_k + (-1)^k k\sigma_k = (-1)^{k+1} \sum_{i=1}^{k-1} (-1)^i \sigma_{k-i}\pi_i \\ 2)\ \text{Si } k > n, \quad \pi_k = (-1)^{k+1} \sum_{i=k-n}^{k-1} (-1)^i \sigma_{k-i}\pi_i \end{array}\right\} \text{[Identidades de Newton]}$$

$\equiv$

Hacemos la demostración por inducción sobre n. Para $n = 1$, tenemos

$$\text{Para } k \leq n \ \rightarrow\ k = 1 \ \rightarrow\ \pi_k + (-1)^k k\sigma_k = \pi_1 - \sigma_1 = x_1 - x_1 = 0$$
$$\overset{(k-1=0)}{=} (-1)^{k+1} \sum_{i=1}^{k-1} (-1)^i \sigma_{k-i}\pi_i$$

$$\text{Para } k > n \ \rightarrow\ (-1)^{k+1} \sum_{i=k-n}^{k-1} (-1)^i \sigma_{k-i}\pi_i$$
$$= (-1)^{k+1}(-1)^{k-1}\sigma_1\pi_{k-1} = x_1^k = \pi_k$$

Luego las identidades valen para $n = 1$. Suponiéndolas válidas para $n - 1$, veamos que valen para n. 1) Si $k \leq n$, distinguimos dos casos

Uno. $k \leq n-1$. Aplicando la hipótesis de inducción,

$$\pi'_k + (-1)^k k\sigma'_k \;=\; (-1)^{k+1}\sum_{i=1}^{k-1}(-1)^i\sigma'_{k-i}\pi'_i, \qquad (*)$$

donde $\sigma'_k(x_1, x_2, ..., x_{n-1}) := \sigma_k(x_1, x_2, ..., 0)$; $\pi'_k := \pi_k(x_1, x_2, ..., 0) = x_1^k + ... + x_{n-1}^k$. Consideremos el polinomio

$$\delta_k(x_1, x_2, ..., x_n) \;:=\; \pi_k - (-1)^{k+1}k\sigma_k + (-1)^{k+1}\sum_{i=1}^{k-1}(-1)^i\sigma_{k-i}\pi_i.$$

Entonces δ_k es un polinomio simétrico tal que, haciendo uso de $(*)$, $\delta_k(x_1, x_2, ..., 0) = 0$. Ello implica que $x_n \mid \delta_k$. Por tanto, al ser simétrico, $\sigma_n = x_1x_2...x_n \mid \delta_k$. Pero, como el grado de σ_n es n y el de δ_k es $k \leq n-1 < n$, deducimos que $\delta_k = 0$, lo que nos da la igualdad deseada.

Dos. $k = n$. Ahora, aplicando la hipótesis inductiva, ya que $n > n-1$, en la igualdad 2), podemos escribir

$$\pi'_n \;=\; (-1)^{n+1}\sum_{i=1}^{n-1}(-1)^i\sigma'_{n-i}\pi'_i.$$

Procediendo como antes, consideramos el polinomio

$$\delta_n(x_1, x_2, ..., x_n) \;:=\; \pi_n \;-\; (-1)^{n+1}\sum_{i=1}^{n-1}(-1)^i\sigma_{n-i}\pi_i,$$

que es simétrico y, análogamente a lo hecho anteriormente, $\sigma_n \mid \delta_n$. De la igualdad de grados, podemos afirmar que exista $c \in F$ (F un cuerpo numérico cualquiera) tal que $\delta_n = c\sigma_n$. En particular, tomando $x_1 = x_2 = ... = x_n = 1$, obtenemos

$$c\;\sigma_n(1, 1, ..., 1) = \delta_n(1, 1, ..., 1)$$

$$\Rightarrow\; c \;=\; \pi_n(1, 1, ..., 1) - (-1)^{n-1}\sum_{i=1}^{n-1}(-1)^i\sigma_{n-i}(1, ..., 1)\pi_i(1, ..., 1)$$

$$= n - (-1)^{n-1}\sum_{i=1}^{n-1}(-1)^i\begin{pmatrix} n \\ i \end{pmatrix}n.$$

Llamando $a_n := \sum_{i=1}^{n-1}(-1)^i\begin{pmatrix} n \\ i \end{pmatrix}$, tenemos que $c = n + (-1)^n n a_n$. Entonces se tiene

$$\left.\begin{array}{l} \text{Si n es par} \rightarrow\; a_n = -2 \;\rightarrow\; c = n - 2n = -n \\ \text{Si n es impar} \rightarrow\; a_n = \rightarrow\; c = n \end{array}\right\} \;\Rightarrow\; c = (-1)^{n+1}n.$$

Por tanto

$$\pi_n \;=\; (-1)^{n+1}n\sigma_n + (-1)^{n+1}\sum_{i=1}^{n-1}(-1)^i\sigma_{n-i}\pi_i.$$

Finalmente, si $k > n$, como $k > n-1$, podemos aplicar la hipótesis de inducción a la segunda identidad para escribir

$$\pi'_k = (-1)^{k+1} \sum_{i=k-n+1}^{k-1} (-1)^i \sigma'_{k-i}\pi'_i \overset{(\sigma'_{k-(k-n)}=\sigma'_n=0)}{=} (-1)^{k+1} \sum_{i=k-n}^{k-1} (-1)^i \sigma'_{k-i}\pi'_i.$$

Considerando

$$\delta_k(x_1, x_2, ..., x_n) := \pi_k - (-1)^{k+1} \sum_{i=1}^{k-1} (-1)^i \sigma_{k-i}\pi_i,$$

procediendo como antes se ve que $\sigma_n \mid \delta_k$, lo que, como $n < k$, obliga a que $\delta_k = 0$. Hemos terminado. ♣

Ex. 260 *Sea $F(x_1, x_2, ..., x_n)$ el cuerpo de las funciones racionales sobre el cuerpo F en las variables $x_1, x_2, ...x_n$. Demostrar que $F(x_1, x_2, ..., x_n)$ es una extensión de Galois de $F(\sigma_1, \sigma_2, ..., \sigma_n)$, donde $\sigma_1, \sigma_2, ..., \sigma_n$ son las funciones elementales de n variables, viendo que su grupo de Galois es isomorfo al grupo simétrico Σ_n.*

≡

Vamos a demostrar que $\mathcal{G}(F_x/F_\sigma)$ es isomorfo a Σ_n, con lo cual tendremos lo que pide el enunciado. Definimos

$$\begin{array}{rccl} f & : & \mathcal{G}(F_x/F_\sigma) & \longrightarrow & \Sigma_n \\ & & \Phi & \to & f(\Phi) := (\Phi(x_1), \Phi(x_2), ..., \Phi(x_n)). \end{array}$$

f bien definido: Dado $\Phi \in \mathcal{G}(F_x/F_\sigma)$, tenemos que ver que, para $i = 1, 2, ..., n$, $\Phi(x_i) \in \{x_1, x_2, ..., x_n\}$. Para ello, consideramos el polinomio

$$(X - x_1)(X - x_2)...(X - x_n) = X^- - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + ... + (-1)^n \sigma_n.$$

Como Φ fija F_σ

$$\begin{array}{l} \sigma_1 = \Phi(\sigma_1) = \Phi(x_1) + \Phi(x_2) + ... + \Phi(x_n) \\ \sigma_2 = \Phi(\sigma_2) = \Phi(x_1)\Phi(x_2) + ... + \Phi(x_{n-1})\Phi(x_n) \\ ..... \\ ..... \\ \sigma_n = \Phi(\sigma_n) = \Phi(x_1)\Phi(x_2)...\Phi(x_n). \end{array}$$

Las ecuaciones anteriores implican, al resolverlas, que $\Phi(x_1), \Phi(x_2), ..., \Phi(x_n)$ son raíces del polinomio anterior. Consecuentemente $\{\Phi(x_1), \Phi(x_2), ..., \Phi(x_n)\} = \{x_1, x_2, ..., x_n\}$.
f homomorfismo de grupos: Dados $\Phi_1, \Phi_2 \in \mathcal{G}(F_x/F_\sigma)$

$$f(\Phi_1 \circ \Phi_2) = ((\Phi_1 \circ \Phi_2)(x_1), (\Phi_1 \circ \Phi_2)(x_2), ..., (\Phi_1 \circ \Phi_2)(x_n))$$

$$= (\Phi_1(\Phi_2(x_1)), \Phi_1(\Phi_2(x_2)), ..., \Phi_1(\Phi_2(x_n))) = f(\Phi_1) \circ f(\Phi_2).$$

f inyectivo: Si $\Phi \in Ker(f)$, entonces

$$Id_{\{x_1,...,x_n\}} = f(\Phi) \Rightarrow \left\{ \begin{array}{l} \Phi(x_1) = x_1 \\ \Phi(x_2) = x_2 \\ ..... \\ ..... \\ \Phi(x_n) = x_n \end{array} \right\}$$

$$\Rightarrow \forall \frac{p(x_1,...,x_n)}{q(x_1,...,x_n)} \in F_x, \Phi(\frac{p(x_1,...,x_n)}{q(x_1,...,x_n)}) = \frac{p(x_1,...,x_n)}{q(x_1,...,x_n)}.$$

Luego $\Phi = Id_{F_x}$.

f sobre: Dada la permutación $\pi \in \Sigma_n$, considerando como conjunto soporte del grupo simétrico a $\{x_1, x_2, ..., x_n\}$, definimos

$$\begin{array}{rcl} \Phi & : & F_x \longrightarrow F_x \\ \frac{p(x_1,...,x_n)}{q(x_1,...,x_n)} & \rightarrow & \Phi(\frac{p(x_1,...,x_n)}{q(x_1,...,x_n)}) := \frac{p(\pi(x_1),...,\pi(x_n))}{q(\pi(x_1),...,\pi(x_n))}. \end{array}$$

Es inmediato comprobar que Φ es un automorfismo del cuerpo F_x. Veamos para terminar que Φ fija F_σ: Basta con verificar que, si $i = 1, 2, ..., n$, entonces $\Phi(\sigma_i) = \sigma_i$

$$\Phi(\sigma_1) = \Phi(x_1 + x_2 + ... + x_n) = \pi(x_1) + \pi(x_2) + ... + \pi(x_n)$$
$$\stackrel{(\pi \ biyect.)}{=} x_1 + x_2 + ... + x_n = \sigma_1$$

$$\Phi(\sigma_2) = \Phi(x_1x_2 + ... + x_{n-1}x_n) = \pi(x_1)\pi(x_2) + ... + \pi(x_{n-1}\pi(x_n)$$
$$\stackrel{(\pi \ biy.)}{=} x_1x_2 + ... + x_{n-1}x_n = \sigma_2$$
$$.....$$
$$.....$$
$$\Phi(\sigma_n) = \Phi(x_1x_2...x_n) = \pi(x_1)\pi(x_2)...\pi(x_n) \stackrel{(\pi \ biyect.)}{=} x_1x_2...x_n = \sigma_n$$

Por tanto, $\Phi \in \mathcal{G}(F_x/F_\sigma)$ y $f(\Phi) = \pi$. ♣

Ex. 261 *Sea $f(x) \in \mathbf{Q}[x]$ tal que no tiene raíces repetidas. Sea E su cuerpo raíz en $\mathbf{C}$. Demostrar que $Gal(E/\mathbf{Q})$ actúa trnsitivamente sobre el conjunto de las raíces de $f(x)$ si y sólo si $f(x)$ es irreducible sobre $\mathbf{Q}$.*

$\equiv$

[$\Rightarrow$] Sea $grado(f(x)) = n$ y $f(x) = c(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$, con $\alpha_1, \alpha_2, ..., \alpha_n$ todas distintas. Supongamos que existe $g(x) = a_0 + a_1x + ... + x^m \in \mathbf{Q}[x]$, con $m \geq 1$, tal que $g(x)$ es divisor de $f(x)$. Entonces, como $g(x)$ no es constante, existe alguna raíz α_i tal que $g(\alpha_i) = 0$. Como por hipótesis $Gal(E/\mathbf{Q})$ actúa transitivamente sobre esas raíces, para cada $j = 1, 2, ..., n$, existe $\Phi \in Gal(E/\mathbf{Q})$ tal que $\Phi(\alpha_i) = \alpha_j$. Entonces

$$g(\alpha_j) = \sum_{h=0}^{m} a_h\alpha_j^h = \sum_{h=0}^{m} a_h\Phi(\alpha_i)^h = \Phi(\sum_{h=0}^{m} a_h\alpha_i^h) = \Phi[g(\alpha_i)] = \Phi(0) = 0.$$

Ello implica que $g(x)$ tiene las mismas raíces que $f(x)$, es decir, $g(x)$ es un múltiplo racional de $f(x)$, lo que prueba la irreducibilidad de $f(x)$.
$[\Leftarrow]$ Suponiendo que $Gal(E/\mathbf{Q})$ no actúa transitivamente sobre el conjunto $\{\alpha_1, \alpha_2, ..., \alpha_n\}$, entonces existen $\alpha_i \neq \alpha_j$ tales que, para todo $\Phi \in Gal(E/\mathbf{Q})$, $\Phi(\alpha_i) \neq \alpha_j$. Consideremos el conjunto

$$\{\alpha_{i_1}, \alpha_{i_2}, ..., \alpha_{i_k}\} \ := \ \{ \ \Phi(\alpha_i) \ : \ \Phi \in Gal(E/\mathbf{Q}) \ \} \ \cap \ \{\alpha_1, \alpha_2, ..., \alpha_n\}$$

y sea

$$g(x) \ := \ (x - \alpha_{i_1})(x - \alpha_{i_2})...(x - \alpha_{i_k}).$$

Como $\alpha_j \notin \{\alpha_{i_1}, \alpha_{i_2}, ..., \alpha_{i_k}\}$, se tiene que $grado(g(x)) < grado(f(x))$. Además

$$g(x) \ = \ x^k - \sigma_1' x^{k-1} + \sigma_2' x^{k-2} + ... + (-1)^k \sigma_k',$$

siendo $\sigma_1' = \alpha_{i_1} + ... + \alpha_{i_k}$, $\sigma_2' = \alpha_{i_1}\alpha_{i_2} + ... + \alpha_{i_{k-1}}\alpha_{i_k}, ..., \sigma_k' = \alpha_{i_1}...\alpha_{i_k}$. Sea ahora Φ un elemento arbitrario de $Gal(E/\mathbf{Q})$. Para cada $h = 1, 2, ..., k$, por definición del conjunto de arriba, existe $\varphi_h \in Gal(E/\mathbf{Q})$ tal que $\varphi_h(\alpha_i) = \alpha_{i_h}$. Así

$$\Phi(\alpha_{i_h}) \ = \ \Phi[\varphi_h(\alpha_i)] \ = \ (\Phi \circ \varphi_h)(\alpha_i) \ \in \ \{\alpha_{i_1}, \alpha_{i_2}, ..., \alpha_{i_k}\}.$$

Se desprende entonces que

$$\Phi(\sigma_1') \ = \ \sigma_1', \ \ \Phi(\sigma_2') \ = \ \sigma_2', \ \ ... \ , \ \Phi(\sigma_k') \ = \ \sigma_k'.$$

Como ese fijamiento se tiene para cualquier $\Phi \in Gal(E/\mathbf{Q})$, deducimos que $\{\sigma_1', \sigma_2', ..., \sigma_k'\} \subset \mathbf{Q}$. Es decir, $g(x) \in \mathbf{Q}[x]$. Como $g(x)$ es un divisor de $f(x)$, ello implica que $f(x)$ no es irreducible sobre $\mathbf{Q}$. ♣

Ex. 262 *Sea $f(x) \in \mathbf{Q}[x]$ un polinomio de grado n. Sea E el cuerpo raíz de $f(x)$ en $\mathbf{C}$. Demostrar que*

$$o(Gal(E/\mathbf{Q})) \ | \ n! \ .$$

≡

Sean $\alpha_1, \alpha_2, ..., \alpha_n$ las raíces de $f(x)$, posiblemente repetidas. Sabemos que $E = \mathbf{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$ es una extensión de Galois de $\mathbf{Q}$ tal que su grupo de Galois $Gal(E/\mathbf{Q})$ es isomorfo a un subgrupo del grupo simétrico Σ_n. Consecuentemente, queda claro que

$$o(Gal(E/\mathbf{Q})) \ | \ o(\Sigma_n) \ = \ n! \ . \ ♣$$

Ex. 263 *Sea $f(x) \in \mathbf{Q}[x]$ un polinomio de grado 8 tal que no tiene raíces en $\mathbf{Q}$ pero es reducible sobre $\mathbf{Q}$. Demostrar que, si E es su cuerpo raíz, entonces $[E : \mathbf{Q}] \leq 1440$.*

≡

Sean $g(x), h(x) \in \mathbf{Q}[x]$ tales que, al no tener raíces racionales, $f(x) = g(x)h(x)$, con $grado(g(x)) = n \geq 2$ y $grado(h(x)) = 8 - n \geq 2$. Si $\alpha_1, \alpha_2, ..., \alpha_8 \in \mathbf{C}$ son las raíces de $f(x)$, sean

$\alpha_1, \alpha_2, ..., \alpha_n$ las raices de g(x)
$\alpha_{n+1}, \alpha_{n+2}, ..., \alpha_8$ las raices de h(x).

Dado $\Phi \in Gal(E/\mathbf{Q})$, como Φ fija $\mathbf{Q}$, se tiene que

$$\Phi(\{\alpha_1, \alpha_2, ..., \alpha_n\}) = \{\alpha_1, \alpha_2, ..., \alpha_n\}$$
$$\Phi(\{\alpha_{n+1}, \alpha_{n+2}, ..., \alpha_8\}) = \{\alpha_{n+1}, \alpha_{n+2}, ..., \alpha_8\}.$$

Por tanto, Φ se identifica con un elemento del grupo producto $\Sigma_n \times \Sigma_{8-n}$. Es decir, $Gal(E/\mathbf{Q})$ es isomorfo a un subgrupo del producto anterior. Así

$$[E : \mathbf{Q}] \;=\; o(Gal(E/\mathbf{Q})) \mid o(\Sigma_n \times \Sigma_{8-n}) \;=\; n! \cdot (8-n)! \;\leq\; 1440,$$

como se puede verificar manualmente tomando valores para $n \in \{2, 3, 4, 5, 6\}$. De hecho, el máximo de dicho producto de factoriales se alcanza en $6! \cdot 2! = 720 \cdot 2 = 1440$. ♣

Ex. 264 *Sea K el cuerpo raíz en $\mathbf{C}$ del polinomio $x^4 - 2$. Sean $\Phi, \varphi \in \mathcal{G}(K)$ tales que*

$$\Phi(\sqrt[4]{2}) = \mathbf{i}\sqrt[4]{2}, \quad \Phi(\mathbf{i}) = \mathbf{i}$$
$$\varphi(\sqrt[4]{2}) = \sqrt[4]{2}, \quad \varphi(\mathbf{i}) = -\mathbf{i}.$$

Demostrar que

$$Gal(K/\mathbf{Q}) \;=\; \{\; Id_k, \Phi, \Phi^2, \Phi^3, \varphi, \Phi\varphi, \Phi^2\varphi, \Phi^3\varphi \;\}.$$

≡

[$\subset$] Si $\eta \in Gal(K/\mathbf{Q})$, como $K = \mathbf{Q}(\sqrt[4]{2}, \mathbf{i})$, tenemos

$$\left.\begin{array}{l} 0 = \eta((\sqrt[4]{2})^4 - 2) = \eta(\sqrt[4]{2})^4 - 2 \;\rightarrow\; \eta(\sqrt[4]{2}) \in \{\pm\sqrt[4]{2}, \pm\mathbf{i}\sqrt[4]{2}\} \\ 0 = \eta(\mathbf{i}^2 + 1) = \eta(\mathbf{i})^2 + 1 \;\rightarrow\; \eta(\mathbf{i}) \in \{\pm\mathbf{i}\} \end{array}\right\},$$

lo que implica que $(\eta(\sqrt[4]{2}), \eta(\mathbf{i})) \in \{\pm\sqrt[4]{2}, \pm\mathbf{i}\sqrt[4]{2}\} \times \{\pm\mathbf{i}\}$. Ello claramente garantiza que η es uno de los 8 elementos del conjunto de arriba.

[$\supset$] Al tratarse de automorfismos de un cuerpo numérico, es evidente que cualquier elemento del conjunto

$$\{\; Id_k, \Phi, \Phi^2, \Phi^3, \varphi, \Phi\varphi, \Phi^2\varphi, \Phi^3\varphi \;\}$$

deja fijo a $\mathbf{Q}$. ♣

Ex. 265 *Si E es el cuerpo raíz de $x^4 + x^2 - 6$ sobre $\mathbf{Q}$, determinar $Gal(E/\mathbf{Q})$.*

≡

Al ser un polinomio bicuadrado

$$x^4 + x^2 - 6 \;=\; (x^2 - 2)(x^2 + 3) \;=\; (x - \sqrt{2})(x + \sqrt{2})(x - \mathbf{i}\sqrt{3})(x + \mathbf{i}\sqrt{3}).$$

Por tanto, $E = \mathbf{Q}(\sqrt{2}, \mathbf{i}\sqrt{3})$. Entonces los elementos de $Gal(E/\mathbf{Q})$ están determinados por sus valores sobre $\{\sqrt{2}, \mathbf{i}\sqrt{3}\}$. Pero, si $\Phi \in Gal(E/\mathbf{Q})$

$$0 = \Phi((\sqrt{2})^2 - 2) = \Phi(\sqrt{2})^2 - 2 \;\rightarrow\; \Phi(\sqrt{2}) \in \{\pm\sqrt{2}\}$$
$$0 = \Phi((\mathbf{i}\sqrt{3})^2 + 3) = \Phi(\mathbf{i}\sqrt{3})^2 + 3 \;\rightarrow\; \Phi(\mathbf{i}\sqrt{3}) \in \{\pm\mathbf{i}\sqrt{3}\}$$

Por tanto

$$(\Phi(\sqrt{2}), \Phi(\mathbf{i}\sqrt{3})) \in \{\pm\sqrt{2}\} \times \{\pm\mathbf{i}\sqrt{3}\}$$

. Definiendo

$$\Phi_1(a + b\sqrt{2} + c\mathbf{i}\sqrt{3}) := a - b\sqrt{2} + c\mathbf{i}\sqrt{3}$$
$$\Phi_2(a + b\sqrt{2} + c\mathbf{i}\sqrt{3}) := a + b\sqrt{2} - c\mathbf{i}\sqrt{3}$$

obtenemos dos automorfismos, de modo que $Gal(E/\mathbf{Q}) = \{Id_E, \Phi_1, \Phi_2, \Phi_1\Phi_2\}$. ♣

Nota 28 Debido a que $x^4 + x^2 - 6 = (x^2 - 2)(x^2 + 3)$, obsérvese que $Gal(E/\mathbf{Q})$ coincide con el producto directo $\{Id_E, \Phi_1\} \times \{Id_E, \Phi_1\}$.

Ex. 266 *Hallar el grupo de Galois de la menor extensión de Galois de* $\mathbf{Q}$ *que contenga a* $\sqrt{2} + \sqrt[3]{2}$.

≡

Sea E la menor extensión de Galois de $\mathbf{Q}$ que contiene a $\sqrt{2}+\sqrt[3]{2}$. Sabemos de ejercicios anteriores que la menor extensión de Galois que contiene $\sqrt[3]{2}$ es $\mathbf{Q}(\sqrt[3]{2}, \zeta)$, con $\zeta = \mathrm{e}^{\frac{2\pi\mathbf{i}}{3}}$. Como $\mathbf{Q}(\sqrt{2}, \sqrt[3]{2}, \zeta)$ es el cuerpo raíz del polinomio $(x^2 - 2)(x^3 - 2)$ sobre $\mathbf{Q}$, tenemos que $E = \mathbf{Q}(\sqrt{2}, \sqrt[3]{2}, \zeta)$. Vamos a hallar el grupo de Galois de E. Sea $\Phi \in Gal(E\mathbf{Q})$. Entonces Φ está determinado por los valores $\Phi(\sqrt{2}), \Phi(\sqrt[3]{2}), \Phi(\zeta)$.

$$0 = \Phi((\sqrt{2})^2 - 2) = \Phi(\sqrt{2})^2 - 2 \;\rightarrow\; \Phi(\sqrt{2}) \in \{\pm\sqrt{2}\}$$
$$0 = \Phi((\sqrt[3]{2})^3 - 2) = \Phi(\sqrt[3]{2})^3 - 2 \;\rightarrow\; \Phi(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\}$$
$$0 = \Phi(\zeta^3 - 1) = \Phi(\zeta)^3 - 1 \;\rightarrow\; \Phi(\zeta) \in \{\zeta, \zeta^2\}.$$

Así, llamando

	$\sqrt{2}$	$\sqrt[3]{2}$	ζ
σ	$-\sqrt{2}$	$\sqrt[3]{2}$	ζ
τ	$\sqrt{2}$	$\zeta\sqrt[3]{2}$	ζ
Φ	$\sqrt{2}$	$\sqrt[3]{2}$	ζ^2 ,

tenemos que

$$Gal(E/\mathbf{Q}) \;=\; \{Id_E, \sigma\} \times \{Id_E, \tau, \tau^2\} \times \{Id_E, \Phi\}.\ \clubsuit$$

Nota 29 Como, en el ejercicio previo, $o(Gal(F/\mathbf{Q}) = 12$, éso nos dice que el grado del polinomio mínimo de $\sqrt{2} + \sqrt[3]{2}$ sobre $\mathbf{Q}$ es 12. Menos mal que no nos lo piden !!!

Ex. 267 *Indicar los grupos de Galois que pueden existir para los cuerpos raíces de ecuaciones cúbicas, dando un ejemplo para cada caso.*

≡

Sea E el cuerpo raíz del polinomio $f(x) = x^3 - px^2 + qx - r \in \mathbf{Q}[x]$. Sean $\alpha_1, \alpha_2, \alpha_3$ las raíces de $f(x)$. Observemos primero que o bien las tres raíces están en $\mathbf{Q}$, o sólo una, o ninguna. Si, por ejemplo, $\alpha_1, \alpha_2 \in \mathbf{Q}$ y $\alpha_3 \notin \mathbf{Q}$, entonces

$$p \;=\; \alpha_1 + \alpha_2 + \alpha_3 in\mathbf{Q} \;\rightarrow\; \alpha_3 \;=\; p - \alpha_1 - \alpha_2 \;\in \mathbf{Q}.\ \text{Absurdo}$$

Por tanto, tenemos tres posibilidades
Una. Las tres raíces están en $\mathbf{Q}$. Entonces, es obvio que $E = \mathbf{Q}$ y $Gal(E/\mathbf{Q}) = \{Id_{\mathbf{Q}}\}$.
Ex. 1: $f(x) = x(x-1)(x-2)$. Es evidente que $E = \mathbf{Q}$.
Dos. Sólo una raíz está en $\mathbf{Q}$. Supongamos que $\alpha_1 \in \mathbf{Q}$ y que $\alpha_2, \alpha_3 \notin \mathbf{Q}$. Ahora $E = \mathbf{Q}(\alpha_2, \alpha_3)$ y sabemos que $Gal(E/\mathbf{Q}) = \Sigma_2$.
Ex. 2: $f(x) = x^3 - 1$. Ahora, $E = \mathbf{Q}(\zeta)$, con $\zeta = \mathrm{e}^{\frac{2\pi \mathrm{i}}{3}}$.
Tres. Ninguna raíz está en $\mathbf{Q}$. El polinomio $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ es irreducible sobre $\mathbf{Q}$, ya que, si $g(x) \in \mathbf{Q}[x]$ es un divisor propio de $f(x)$, entonces $g(x)$ es de la forma $c(x-\alpha_i)$, ó $c(x-\alpha_i)(x-\alpha_j)$, pero ello no puede ser, pues entonces se ve fácilmente que alguna raíz sería racional. Como las tres raíces son distintas, sabemos que $Gal(E/\mathbf{Q}) = \Sigma_3$.
Ex. 3: $f(x) = x^3 - 2$. En este caso, $E = \mathbf{Q}(\sqrt[3]{2}, \zeta)$. ♣

Ex. 268 *Sea $\zeta = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$. Demostrar que, para $d \in \mathbf{N}$, $d \leq n$,*
a) ζ^k es raíz primitiva $(\frac{n}{d})$-ésima de la unidad si y sólo si $mcd(k,n) = d$.
b) Emplear el apartado anterior para demostrar que

$$\Phi_d(x) \;=\; \prod_{mcd(j,d)=1} (x - \zeta^j). \qquad \text{[polinomio ciclotómico d – ésimo]}$$

≡
a)
[⇒] Supongamos que ζ^k es raíz primitiva $(\frac{n}{d})$-ésima de la unidad. Entonces

$$o(\zeta^k) \;=\; \frac{n}{d} \;\to\; \frac{n}{d} \;=\; \frac{o(\zeta)}{mcd(o(\zeta),k)} \;=\; \frac{n}{mcd(n,k)} \;\to\; d = mcd(n,k).$$

[⇐] Si $d = mcd(n,k)$, entonces

$$o(\zeta^k) \;=\; \frac{n}{d} \;\to\; (\zeta^k)^{\frac{n}{d}} \;=\; 1.$$

Además, como $o(\langle\, \zeta^k \,\rangle) = \frac{n}{d}$, se tiene que ζ^k genera a las raíces $(\frac{n}{d})$-ésimas de la iunidad, es decir, ζ^k es una raíz primitiva.
b) Para cada $d \mid n$, consideremos el polinomio ciclotómico d-ésimo

$$\Phi_d(x) \;=\; \prod_{mcd(k,d)=1} (x - \zeta_d^k),$$

donde $\zeta_d = \mathrm{e}^{\frac{2\pi \mathrm{i}}{d}}$. Formamos ahora el polinomio

$$f(x) \;:=\; \prod_{d \mid n} \Phi_d(x).$$

Entonces

$$grado(f) \;=\; \sum_{d \mid n} grado(\Phi_d) \;=\; \sum_{d \mid n} \Phi(d) \;=\; n, \quad \text{donde } \Phi \text{ es la función de Euler.}$$

Al ser del mismo grado, para ver que $f(x) = x^n - 1$, todo se reduce a probar que $f(\zeta^k) = 0$, $1 \leq k \leq n$. Necesitamos observar que

$$\zeta_{n/d}^k \;=\; \mathrm{e}^{k\frac{2\pi \mathrm{i}}{n/d}} \;=\; e^{kd\frac{2\pi \mathrm{i}}{n}} \;=\; \zeta^{kd}.$$

Así

$$f(x) \overset{(simetria\ de\ divisores)}{=} \prod_{d \mid n} \Phi_{\frac{n}{d}}(x) = \prod_{d \mid n} [\prod_{mcd(k,n/d)=1} (x - \zeta_{n/d}^k)] = \prod_{d \mid n} [\prod_{mcd(k,n/d)=1} (x - \zeta^{kd})]$$

$$= \prod_{d \mid n} [\prod_{mcd(kd,n)=1} (x - \zeta^{kd})] = \prod_{d \mid n} [\prod_{mcd(k,n)=d} (x - \zeta^k)].$$

Finalmente, para $k = 1, 2, ..., n$, sea $d := mcd(k, n)$. Entonces $d \mid n$ y $f(x)$ contiene como factor a $x - \zeta^k$. Por lo tanto, $f(\zeta^k) = 0$. ♣

Ex. 269 *Hacer uso de la fórmula* $x^n - 1 = \prod_{d|n} \Phi_d(x)$ *para clacular* $\Phi_n(x)$, $1 \leq n \leq 10$.

≡

Primero notemos que, para p primo, $\Phi_p(x) = x^{p-1} + x^{p-2} + ... + x + 1$. La siguiente tabla resuelve el ejercicio, como siempre Φ es la función de Euler,

n	$\Phi_n(x)$	$\Phi(n)$	
1	$x - 1$	1	
2	$x + 1$	1	
3	$x^2 + x + 1$	2	
4	$x^2 + 1$	2	$[\Leftarrow\ x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)]$
5	$x^4 + x^3x^2 + x + 1$	4	
6	$x^2 - x + 1$	2	$[\Leftarrow\ x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)]$
7	$x^6 + x^5x^4 + x^3x^2 + x + 1$	6	
8	$x^4 + 1$	4	$[\Leftarrow\ x^8 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)]$
9	$x^6 + x^3 + 1$	6	$[\Leftarrow\ x^9 - 1 = \Phi_1(x)\Phi_3(x)\Phi_9(x)]$
10	$x^4 - x^3 + x^2 - x + 1$	4	$[\Leftarrow\ x^{10} - 1 = \Phi_1(x)\Phi_2(x)\Phi_5(x)\Phi_{10}(x)]$. ♣

Ex. 270

a) Dados $m, n \in \mathbf{N}$ *tales que, si* p *primo divide a* m, *entonces* p *divide a* n. *Demostrar que*

$$\Phi_{mn}(x) \;=\; \Phi_n(x^m).$$

b) Aplicando lo anterior, calcular Φ_{24}, Φ_{36}, Φ_{100}.

≡

a) Necesitamos un resultado auxiliar relativo a la función de Euler.

Lema 9 *Si* m, n *son como antes, entonces* $\Phi(mn) = m\Phi(n)$.

$\equiv$

Observar que, por la definición de la función Φ, que cuenta todos los números anteriores que son primos con el dado, todo se reduce a demostrar que: $mcd(k, mn) = 1 \Leftrightarrow \exists r \in \{0, 1, ..., m-1\}, \exists j \ / \ mcd(j, n) = 1$ tales que $k = rn + j$.

$[\Rightarrow]$ Sea $k < mn$ tal que $mcd(k, mn) = 1$. Haciendo la división entera, existen r, j tales que

$$\begin{array}{l} k = rn + j \\ k < mn \rightarrow \ 0 \leq r \leq m-1 \\ 0 \leq j < n. \end{array}$$

Entonces

$$\text{como } mcd(k, mn) = 1 \overset{(Bezout)}{\rightarrow} \ 1 = ak + bmn = arn + aj + bmn = aj + (ar + bm)n$$

$$\rightarrow \ mcd(j, n) = 1.$$

$[\Leftarrow]$ Si $k = rn + j$, $0 \leq m-1$, $mcd(j, n) = 1$, entonces

$$1 = aj + bn = a(k - rn) + bn = ak + (b - ar)n \ \rightarrow \ mcd(k, n) = 1.$$

Si $mcd(k, mn) \neq 1$, del lema de Euclides, k sería divisor de m; ello implica que algún primo dividirá a m, pero, por hipótesis ese primo también dividiría a n, lo que es absurdo ya que k y n son primos entre sí. •

Volviendo al ejercicio, de un ejercicio anterior sabemos que

$$x^{mn} - 1 \ = \ \Phi_{mn}(x) \cdot \prod_{d|mn, \ d<mn} \Phi_d(x).$$

Pero

$$x^{mn} - 1 \ = \ (x^m)^n - 1 \ = \ \Phi_n(x^m) \ = \ \Phi_n(x^m) \cdot \prod_{d|n, \ d<n} \Phi_d(x^m).$$

Consideremos los polinomios

$$f(x) \ := \prod_{d|mn, \ d<mn} \Phi_d(x); \quad g(x) \ := \prod_{d|n, \ d<n} \Phi_d(x^m).$$

Claramente, todo consiste en ver que $f(x) = g(x)$. Para empezar, miremos grados

$$grado(f(x)) = \textstyle\sum_{d|mn, \ d<mn} \Phi(d) \overset{(ej. \ result.)}{=} mn - \Phi(mn) \overset{(Lema)}{=} m(n - \Phi(n))$$

$$grado(g(x)) = \textstyle\sum_{d|n, \ d<n} grado[\Phi_d(x^m) = \sum_{d|n, \ d<n} m\Phi(d)$$
$$= m \textstyle\sum_{d|n, \ d<n} \Phi(d) = m(n - \Phi(n)).$$

Ahora miremos raíces

$$g(\alpha) = 0 \ \rightarrow \ \exists d|n, \ d < n, \ \Phi_d(\alpha) = 0$$

$$\rightarrow \exists k < d,\ mcd(k,d) = 1,\ \alpha^m = \zeta_d^k \overset{(n=dr)}{\rightarrow} \alpha = e^{\frac{2\pi i}{mn}r}.$$

Así $\alpha = \zeta_{mn}^{kr}$, de donde $f(\alpha) = 0$. Consecuentemente, al ser polinomios del mismo grado con las mismas raíces (y mónicos, claro), se tiene que $f(x) = g(x)$, como se quería.
b)

$$\begin{aligned}\Phi_{36}(x) &= \Phi_6(x^6) = x^{12} - x^6 + 1\\ \Phi_{100}(x) &= \Phi_{10}(x^{10}) = x^{40} - x^{30} + x^{20} - x^{10} + 1\\ \Phi_{24}(x) &= \Phi_6(x^4) = x^8 - x^4 + 1. \clubsuit\end{aligned}$$

Ex. 271 *Sea b impar y $\zeta = e^{\frac{2\pi i}{n}}$. Demostrar que $\mathbf{Q}(\zeta)$ contiene a todas las raíces $2n$-ésimas de la unidad.*

$\equiv$

Para $k = 0, 1, ..., 2n-1$, hay que ver que $\omega_k := e^{\frac{2\pi i}{2n}k} \in \mathbf{Q}(\zeta)$. Distinguimos dos posibilidades
Una. k es par. Entonces, si $k = 2m$,

$$\omega_k = e^{\frac{2\pi i}{2n}k} = e^{\frac{2\pi i}{n}m} = \zeta^m \in \mathbf{Q}(\zeta).$$

Dos. k es impar. Ahora, si $k = 2m+1$,

$$\omega_k = e^{\frac{2\pi i}{2n}k} = e^{\frac{2\pi i}{n}m} \cdot e^{\frac{\pi i}{n}} = \zeta^m \cdot e^{\frac{\pi i}{n}}.$$

Pero

$$\zeta^{\frac{n+1}{2}} = e^{\frac{2\pi i}{n}\frac{n+1}{2}} = e^{\pi i} \cdot e^{\frac{\pi i}{n}} = -e^{\frac{\pi i}{n}}.$$

De donde

$$\omega_k = \zeta^m \cdot e^{\frac{\pi i}{n}} = \zeta^m \cdot (-\zeta^{\frac{n+1}{2}}) = -\zeta^{m+\frac{n+1}{2}} \in \mathbf{Q}(\zeta),$$

pues, al ser n impar, $\frac{n+1}{2}$ es entero. $\clubsuit$

Ex. 272 *Si n es impar, $n \geq 3$, demostrar que $\Phi_{2n}(x) = \Phi_n(-x)$.*

$\equiv$

Lo hacemos por inducción fuerte sobre n. Par $n = 3$, la cosa es evidente, ya que, como ya vimos,

$$\Phi_6(x) = x^2 - x + 1 = (-x)^2 + (-x) + 1 = \Phi_3(-x).$$

Suponiéndolo cierto para todo impar menor que el impar n, veámoslo para n. Primero observemos que, si D_k representa al conjunto de naturales divisores de k, entonces $D_{2n} = D_n \cup 2D_n$. Así

$$\begin{aligned}\Phi_{2n}(x) &= \frac{x^{2n}-1}{\prod_{d|2n,\ d<2n}\Phi_d(x)} = \frac{x^n-1}{\prod_{d|n}\Phi_d(x)} \cdot \frac{x^n+1}{\prod_{d|n,\ d<n}\Phi_{2d}(x)}\\ &= \frac{x^n+1}{\prod_{d|n,\ d<n}\Phi_{2d}(x)} \overset{(hip.ind.\, d|n \rightarrow d\ impar)}{=} \frac{x^n+1}{(x+1)\prod_{d|n,\ 1<d<n}\Phi_d(-x)}\\ &= \frac{-x^n-1}{(-x-1)\prod_{d|n,\ 1<d<n}\Phi_d(-x)} \overset{(\Phi_1(-x)=-x-1)}{=} \frac{(-x)^n-1}{\prod_{d|n,\ d<n}\Phi_d(-x)} = \Phi_n(-x). \clubsuit\end{aligned}$$

Nota 30 Notar que la igualdad del ejercicio previo no se cumple para el impar 1:

$$\begin{array}{rcl} \Phi_2(x) & = & x+1 \\ \Phi_1(-x) & = & (-x)-1 \ = \ -x-1. \end{array}$$

Ex. 273 *Demostrar que, si ω es una raíz n-ésima de la unidad, entonces*

$$1+\omega+\omega^2+...+\omega^{n-1} \ = \ \begin{cases} n, & \text{si } \omega = 1, \\ 0, & \text{si } \omega \neq 1. \end{cases}$$

≡

Para $\omega = 1$, la igualdad es obvia. Si $\omega \neq 1$, entonces, como $\omega^n = 1$,

$$1+\omega+\omega^2+...+\omega^{n-1} \ = \ \frac{\omega^n - 1}{\omega - 1} \ = \ 0. \ \clubsuit$$

Ex. 274 *Para $r \in \mathbf{Q}$, hallar* $[\mathbf{Q}(\cos 2\pi r) : \mathbf{Q}]$.

≡

Escribimos $r \in \mathbf{Q}$ como $r = u + \frac{m}{n}$, con $u \in \mathbf{Z}$, $m, n \in \mathbf{N}$, $0 \leq m < n$, $mcd(m,n) = 1$. Si $m = 0$, ó, $n \in \{1,2\}$, es evidente que $\cos 2\pi r \in \{\pm 1\}$ y entonces $\mathbf{Q}(\cos 2\pi r) = \mathbf{Q}$, de lo que $[\mathbf{Q}(\cos 2\pi r) : \mathbf{Q}] = 1$. Así pues, suponemos que $m \geq 1$ y que $n \geq 3$. Sea $\zeta := e^{\frac{2\pi i}{n}}$. Puesto que

$$Gal(\mathbf{Q}(\cos 2\pi r)/\mathbf{Q}) \ = \ Gal(\mathbf{Q}(\zeta)/\mathbf{Q})/Gal(\mathbf{Q}(\zeta)/\mathbf{Q}(\cos 2\pi r)),$$

vamos a determinar $Gal(\mathbf{Q}(\zeta)/\mathbf{Q}(\cos 2\pi r))$. Fijémonos en que

$$\cos 2\pi r \ = \ \cos \frac{2\pi m}{n} \ = \ \frac{\zeta^m + \zeta^{n-m}}{2}.$$

Entonces, si $\varphi \in Gal(\mathbf{Q}(\zeta)/\mathbf{Q}(\cos 2\pi r))$, como φ deja fijo a $\cos 2\pi r$

$$\begin{array}{l} \exists k \in \mathbf{N}, \ mcd(k,n) = 1, \ \varphi(\zeta) = \zeta^k \\ \cos 2\pi r = \varphi(\cos 2\pi r) \ \rightarrow \ \zeta^m \zeta^{n-m} = \zeta^{mk} + \zeta^{(n-m)k}. \end{array}$$

Ello implica que

$$\cos(\frac{2\pi m}{n}) \ = \ \cos(\frac{2\pi mk}{n}).$$

Por tanto

$$0 \ = \ \cos(\frac{2\pi m}{n}) \ - \ \cos(\frac{2\pi mk}{n}) \ = \ -2 \ \sin(\frac{\pi m(k+1)}{n}) \sin(\frac{\pi m(k-1)}{n}).$$

Ello plantea dos posibilidades
Una. $\sin(\frac{\pi m(k+1)}{n}) = 0$. Entonces

$$\frac{\pi m(k+1)}{n} \ \in \pi\mathbf{Z} \ \rightarrow \ n \mid m(k+1) \ \overset{(mcd(k,n)=1)}{\rightarrow} \ n \mid k+1 \ \overset{(k<n)}{\Rightarrow} \ n = k+1 \ \rightarrow \ k = n-1.$$

Dos. $\sin(\frac{\pi m(k-1)}{n}) = 0$. Entonces

$$\frac{\pi m(k-1)}{n} \in \pi\mathbf{Z} \rightarrow n \mid m(k-1) \overset{(mcd(k,n)=1)}{\rightarrow} n \mid k-1 \overset{(k\leq n)}{\rightarrow} k-1=0 \rightarrow k=1.$$

Resumiendo, tenemos que $\varphi(\zeta) = \zeta$, ó, $\varphi(\zeta) = \zeta^{n-1}$. Consecuentemente, si llamamos φ al automorfismo tal que $\varphi(\zeta) = \zeta^{n-1}$, resulta que

$$Gal(\mathbf{Q}(\zeta)/\mathbf{Q}(\cos 2\pi r)) = \{ Id_{\mathbf{Q}(\zeta)}, \varphi \}.$$

Por lo tanto

$$[\mathbf{Q}(\cos 2\pi r) : \mathbf{Q}] = o(Gal(\mathbf{Q}(\cos 2\pi r)/\mathbf{Q})) = \frac{o(Gal(\mathbf{Q}(\zeta)/\mathbf{Q})}{o(Gal(\mathbf{Q}(\zeta)/\mathbf{Q}(\cos 2\pi r)))} = \frac{\Phi(n)}{2}. \clubsuit$$

Nota 31 Observar que, para $n \geq 3$, $\Phi(n)$ es siempre par. Esta afirmación puede demostrarse inductivamente: Para $n = 3$, sabemos que $\Phi(3) = 2$, claramente par. Suponiendo que la afirmación vale para todo natural menor que n, lo demostramos para n

$$\left.\begin{array}{l} n \text{ par} \rightarrow n = \Phi(1) + \Phi(2) + \sum_{d|n,\ 3\leq d<n} \Phi(d) + \Phi(n) \\ \rightarrow \Phi(n) = n - 2 - \sum_{d|n,\ 3\leq d<n} \Phi(d) \\ \\ n \text{ impar} \rightarrow n = \Phi(1) + \sum_{d|n,\ 3\leq d<n} \Phi(d) + \Phi(n) \\ \rightarrow \Phi(n) = n - 1 - \sum_{d|n,\ 3\leq d<n} \Phi(d) \end{array}\right\}$$

$$\overset{(hip.ind.)}{\Rightarrow} \begin{cases} \Phi(n) \text{ par} \\ \Phi(n) \text{ par.} \end{cases}$$

Ex. 275 *Demostrar que el polinomio ciclotómico satisface la igualdad*

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})},$$

donde μ es la función de Möbius

$$\mu(1) = 1,$$
$$\mu(n) = \begin{cases} 0 & si\ \exists p \text{ primo},\ p^2|n, \\ (-1)^k, & si\ n = p_1 p_2 ... p_k \text{ (primos distintos.} \end{cases}$$

≡

Primero creemos intereante ver algunas propiedades de esta función de Möbius.

Lema 10 *1) Si $n > 1$, entonces $\sum_{d|n} \mu(d) = 0$.*
2) Si $n > 1$ y $m|n$, $m < n$, entonces $\sum_{m|d|n} \mu(\frac{n}{d}) = 0$.
3) Si $mcd(m, n) = 1$, entonces $\mu(mn) = \mu(m)\mu(n)$.
4) $\Phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$.

$\equiv$

1) Sea $n = p_1^{n_1}...p_k^{n_k}$ la descomposición de n en factores primos.

$$\sum_{d|n} \mu(d) = \sum_{1 \le i_1 < i_2 < ... < i_q \le k} \mu(p_{i_1}...p_{i_q}) + \mu(1)$$

$$= \binom{k}{0}(-1)^0 + \binom{k}{1}(-1)^1 + ... + \binom{k}{k}(-1)^k = (1-1)^k = 0.$$

2) $m \mid d \mid n \;\leftrightarrow\; (\frac{n}{d}) \mid (\frac{n}{m})$. Por tanto

$$\sum_{m|d|n} \mu(\frac{n}{d}) \;=\; \sum_{d|(\frac{n}{m})} \mu(\frac{n}{d}) \overset{(prop,1)}{=} 0.$$

3) Sea $m = q_1^{m_1}...q_r^{m_r}$ la descomposición de m en factores primos de modo que $q_i \neq p_j$, $1 \le i \le r$, $1 \le j \le k$. Dos posibilidades

Una. Existe $i \in \{1, 2, ..., r\}$ tal que $m_i > 1$, ó, existe $j \in \{1, 2, ..., k\}$ tal que $n_j > 1$. Entonces

$$\begin{aligned} \mu(mn) &= 0 \\ \mu(m)\mu(n) &= 0. \end{aligned}$$

Dos. $\forall i \in \{1, 2, ..., r\}$, $\forall j \in \{1, 2, ..., k\}$, $m_i = n_j = 1$. Ahora

$$\begin{aligned} \mu(mn) &= \mu(p_1...p_k q_1...q_r) = (-1)^{k+r} \\ \mu(m)\mu(n) &= \mu(p_1...p_k)\mu(q_1...q_r) = (-1)^k(-1)^r. \end{aligned}$$

4)

$$\sum_{d|n} \mu(d)(\frac{n}{d}) = \sum_{p_{i_1} < ... < p_{i_h}} (-1)^h \frac{n}{p_{i_1}...p_{i_h}}$$

$$= (-1)^0 n + (-1)(\frac{n}{p_1} + ... + \frac{n}{p_k}) + (-1)^2(\frac{n}{p_1 p_2} + ... + \frac{n}{p_{k-1}p_k}) + ... + (-1)^k \frac{n}{p_1...p_k}$$

$$= n(1 - \frac{1}{p_1} - ... - \frac{1}{p_k} + \frac{1}{p_1 p_2} + ... + \frac{1}{p_{k-1}p_k} - ... - (-1)^k \frac{1}{p_1...p_k}) = n(1-\frac{1}{p_1})...(1-\frac{1}{p_k}) = \Phi(n). \bullet$$

Volviendo a nuestro ejercicio, sea $f(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$. Como

$$grado(f(x)) \;=\; \sum_{d|n} d \cdot \mu(\frac{n}{d}) \overset{(prop,4)}{=} \Phi(n) \;=\; grado(\Phi_n(x)),$$

todo se reduce a ver que tienen las mismas raíces. Si $f(\alpha) = 0$, entonces $D_\alpha := \{d \in \mathbf{N} : d|n,\ \alpha^d = 1\} \neq \emptyset$ y $\sum_{d \in D_\alpha} \mu(n/d) = 1$, ya que α es raíz de $f(x)$. Pero, si $m := min D_\alpha$, entonces m es el orden de α en $f(x)$, $D_\alpha = \{d \in \mathbf{N} : m|d|n\}$ y

$$1 = \sum_{d \in D_\alpha} \mu(\frac{n}{d}) = \sum_{m|d|n} \mu(\frac{n}{d}).$$

De la propiedad 2) tenemos que $m = n$, es decir, $D_\alpha = \{n\}$. Así, α es una raíz n-ésima de la unidad de orden n, i.e., α es una raíz primitiva n-ésima y por ello $\Phi_n(\alpha) = 0$. $\clubsuit$

Ex. 276 *Empleando resultados de ejercicios anteriores, hallar los polinomios ciclotómicos* $\Phi_n(x)$, $11 \leq n \leq 36$.

$\equiv$

Los polinomios ciclotómicos requeridos se hallan en la siguiente tabla. Las explicaciones acerca de cómo calcularlos están después.

n	$\Phi_n(x)$	$\Phi(n)$
11	$x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x-1$	10
12	x^4-x^2+1	4
13	$x^{12}+...+x+1$	12
14	$x^6-x^5+x^4-x^3+x^2-x+1$	6
15	$x^8-x^7+x^6-x^5+x^4-x^3+x^2-x+1$	8
16	x^8+1	8
17	$x^{16}+...+1$	16
18	x^6-x^3+1	6
19	$x^{18}+...+1$	18
20	$x^8-x^6+x^4-x^2+1$	8
21	$x^{12}-x^{11}+...-x+1$	12
22	$x^{10}-x^9+...-x^2+1$	10
23	$x^{22}+...+1$	22
24	x^8-x^4+1	8
25	$x^{20}+x^{15}+x^{10}+x^5+1$	20
26	$x^{12}-x^{11}+...-x+1$	12
27	$x^{18}+x^9+1$	18
29	$x^{28}+..+1$	28
30	$x^8+x^7+...+x+1$	8
31	$x^{30}+...+1$	30
32	$x^{16}+1$	16
33	$x^{20}-x^{19}+...-x+1$	20
34	$x^{16}-x^{15}+...-x+1$	16
35	$x^{24}-x^{23}+...-x+1$	24
36	$x^{12}-x^6+1$	12.

Haciendo uso de propiedades vistas en ejercicios anteriores, obtenemos los polinomios ciclotómicos pedidos

$$\begin{aligned}
\Phi_{12}(x) &= \Phi_6(x^2)\\
\Phi_{14}(x) &= \Phi_7(-x)\\
\Phi_{15}(x) &= (x-1)^{\mu(15)}(x^3-1)^{\mu(5)}(x^5-1)^{\mu(3)}(x^{15}-1)^{\mu(1)} = \tfrac{(x-1)(x^{15}-1)}{(x^3-1)(x^5-1)}\\
\Phi_{16}(x) &= \Phi_8(x^2)\\
\Phi_{18}(x) &= \Phi_6(x^3)\\
\Phi_{20}(x) &= \Phi_{10}(x^2)\\
\Phi_{21}(x) &= (x-1)^{\mu(21)}(x^3-1)^{\mu(7)}(x^7-1)^{\mu(3)}(x^{21}-1)^{\mu(1)} = \tfrac{(x-1)(x^{21}-1)}{(x^3-1)(x^7-1)} = \tfrac{(x^7)^2+x^7+1}{x^2+x+1}\\
\Phi_{22}(x) &= \Phi_{11}(-x)\\
\Phi_{24}(x) &= \Phi_{12}(x^2)\\
\Phi_{25}(x) &= \Phi_5(x^5)\\
\Phi_{26}(x) &= \Phi_{13}(-x)\\
\Phi_{27}(x) &= \Phi_9(x^3)\\
\Phi_{28}(x) &= \Phi_{14}(x^2)\\
\Phi_{30}(x) &= \Phi_{15}(-x)\\
\Phi_{32}(x) &= \Phi_{16}(x^2)\\
\Phi_{33}(x) &= (x-1)^{\mu(33)}(x^3-1)^{\mu(11)}(x^{11}-1)^{\mu(3)}(x^{33}-1)^{\mu(1)} = \tfrac{(x-1)(x^{33}-1)}{(x^3-1)(x^{11}-1)} = \tfrac{(x^{11})^2+x^{11}+1}{x^2+x+1}\\
\Phi_{34}(x) &= \Phi_{17}(-x)\\
\Phi_{35}(x) &= (x-1)^{\mu(35)}(x^5-1)^{\mu(7)}(x^7-1)^{\mu(5)}(x^{35}-1)^{\mu(1)} = \tfrac{(x-1)(x^{35}-1)}{(x^5-1)(x^7-1)}\\
&= \tfrac{(x^7)^4+(x^7)^3+(x^7)^2+x^7+1}{x^4+x^3+x^2+x+1}\\
\Phi_{36}(x) &= \Phi_6(x^6). \clubsuit
\end{aligned}$$

Ex. 277 *Enumerar los polígonos regulares de n lados,* $3 \leq n \leq 100$*, que son construibles con regla y compás.*

≡

Empleando el resultado que dice: *Un polígono regular de n lados es construible con regla y compás si y sólo si* $\Phi(n)$ *es potencia de* 2. A continuación listamos todos los

polígonos regulares de n lados, $3 \leq n \leq 100$, que son construibles.

n	$\Phi(n)$
3	2
4	2
5	2^2
6	2
8	2^2
10	2^2
12	2^2
15	2^3
16	2^3
17	2^4
20	2^3
24	2^3
30	2^3
32	2^4
34	2^4
40	2^4
48	2^4
51	2^5
60	2^4
64	2^5
68	2^5
80	2^5
85	2^6
96	2^5.

En total hay 24 polígonos regulares construibles con regla y compás de menos de 100 lados. ♣

Ex. 278 *Suponiendo que los polígonos regulares de m y n lados son construibles con regla y compás, demostrar que el polígono de $mcm(m,n)$ lados también es construible.*

≡

Como $\Phi(n)$ es potencia de 2, sea $\Phi(n) = 2^r$. Si $n = 2^{n_0}p_1^{n_1}...p_k^{n_k}$ es la factorización de n en factores primos con $p_1, ..., p_k$ distintos de 2, entonces

$$2^r = \Phi(2^{n_0}) \cdot \prod_{i=1}^{k} \Phi(p_i^{n_i}) = 2^{n_0-1} \cdot \prod_{i=1}^{k} p_i^{n_i-1}(p_i - 1).$$

Así, $\prod_{i=1}^{k} p_i^{n_i-1}(p_i - 1)$ es potencia de 2 y por tanto

$\forall i = 1, 2, ..., k,\ p_i^{n_i-1} \mid 2 \rightarrow n_i = 1 \rightarrow n = 2^{n_0}p_1...p_k,\ \Phi(p_i)$ es potencia de 2, $1 \leq i \leq k$.

Análogamente, como $\Phi(m)$ es potencia de 2, podemos factorizar $m = 2^{m_0}q_1...q_h$, con $q_1, ..., q_h$ primos diferentes de 2 y tales que $\Phi(q_j)$ es potencia de 2, $1 \leq j \leq h$. Entonces, si al unir los conjuntos $\{p_1, ..., p_k\}$ y $\{q_1, ..., q_h\}$ obtenemos el conjunto de primos distintos de 2 dado por $\{r_1, ..., r_s\}$, tenemos que, si $a := \text{máx}\{n_0, m_0\}$,

$$mcm(m,n) = 2^a\, r_1...r_s \Rightarrow \Phi(mcm(m,n)) = 2^{a-1}\prod_{i=1}^{s}\Phi(r_i) \text{ es potencia de 2.}$$

Consecuentemente, el polígono regular de lados $mcm(m,n)$ es construible. ♣

3.4. Resolubilidad de ecuaciones

Ex. 279 *Sea E una extensión de Galois de un cuerpo numérico F que cumple que, dados dos cuerpos intermedios K_1 y K_2 entre F y E, se tiene que, o bien $K_1 \subset K_2$, o bien $K_2 \subset K_1$. Demostrar que E es una extensión radical de F.*

≡

Antes de todo, recordemos el concepto de extensión radical. Dado un cuerpo F, se dice que E es una extensión radical de F siempre que se trate de una extensión finita $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$ tal que existen $k_1, k_2, ..., k_n \in \mathbf{N}$ de modo que

$$\begin{array}{l}
\alpha_1^{k_1} \in F \\
\alpha_2^{k_2} \in F(\alpha_1) \\
\alpha_3^{k_3} \in F(\alpha_1, \alpha_2) \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\alpha_n^{k_n} \in F(\alpha_1, ..., \alpha_{n-1})
\end{array}$$

El siguiente resultado teórico es fundamental pues proporciona una caracterización de las extensiones radicales: *Dado un cuerpo F de característica cero, una extensión de Galois E de F es una extensión radical si y sólo si el grupo de Galois $Gal(E/F)$ es un grupo resoluble.* Observemos que después de leer estas definiciones y resultados se comprende perfectamente el porqué se llaman resolubles a los grupos resolubles (no estaría de más echar una ojeada a la sección de grupos de este tipo).

Volviendo al ejercicio, como F tiene característica cero (al ser un cuerpo numérico) podemos aplicar el resultado anterior. Así, como todo grupo cíclico es resoluble, bastará con ver que $Gal(E/F)$ es cíclico. Para ello, haciendo uso de un problema resuelto de la parte de grupos, es suficiente con ver que, si H_1 y H_2 son dos subgrupos de $Gal(E/F)$, entonces $H_1 \subset H_2$, ó $H_2 \subset H_1$. Del $TFTG$, llamando K_1 y K_2 al cuerpo fijo de H_1 y de H_2, respectivamente, sabemos que, por hipótesis, $K_1 \subset K_2$, ó $K_2 \subset K_1$. Suponiendo que se tiene la primera de las inclusiones, entonces

$$H_2 = G(E/K_2) \overset{(K_2 \supset K_1)}{\subset} G(E/K_1) = H_1. \clubsuit$$

Ex. 280 *Sea E una extensión de Galois de un cuerpo numérico F tal que $Gal(E/F)$ es abeliano. Demostrar que E es extensión radical de F.*

≡

Evidente, aplicando el resultado teórico citado antes, ya que $Gal(E/F)$, al ser un gupo finito abeliano, es resoluble. ♣

Ex. 281 *Sea $f(x) = 0$ una ecuación polinómica de sexto grado que es resoluble por radicales. Demostrar que $f(x) = 0$ sólo es resoluble mediante raíces cuadradas, cúbicas y quintas.*

≡

Primero recordemos lo que significa que una ecuación polinómica sea resoluble por radicales. Dado un cuerpo F, una ecuación polinómica $f(x) = 0$, con $f(x) \in F[x]$, es resoluble por radicales sobre F siempre que exista una extensión radical E de F en donde el polinomio $f(x)$ se descompone.

Así, como $F(x) = 0$ es resoluble por radicales, sea E el cuerpo raíz de $f(x)$ sobre F. Al ser E una extensión radical de F, sabemos que es de Galois y que $Gal(E/F)$ es resoluble. Es más, al ser de grado 6 el polinomio $f(x)$, $Gal(E/F)$ es (isomorfo, realmente) un subgrupo del grupo simétrico Σ_6. Como $o(\Sigma_6) = 6! = 720 = 2^4 \cdot 3^2 \cdot 5$, entonces $Gal(E/F)$ tiene una serie de composición

$$\{e\} = H_0 \preceq H_1 \preceq H_2 \preceq ... \preceq H_n = Gal(E/F)$$

que, al ser una serie normal maximal, cumple que, para cada $i = 1, 2, ..., n$, H_i/H_{i-1} es un grupo cíclico de orden perteneciente al conjunto $\{2, 3, 5\}$. Para cada $i = 0, 1, ..., n-1$, sea K_i el cuerpo fijo de H_{n-i}. Entonces K_{i+1} es una extensión radical de K_i de grado

$$\begin{aligned}[K_{i+1} : K_i] &= o(Gal(K_{i+1}/K_i)) = o(Gal(E/K_i)/Gal(E/K_{i+1})) \\ &= o(H_{n-i}/H_{n-i-1}) \in \{2, 3, 5\}.\end{aligned}$$

Por tanto, para cada $i = 0, 1, ..., n-1$, K_i es extremo final de una torre radical de cuerpos que son cuerpos raíz de polinomios de la forma $x^{m_i} - \alpha_i$, con $\alpha_i \in K_i$ y $m_i \in \{2, 3, 5\}$. Ello prueba lo deseado. ♣

Ex. 282 *Demostrar que toda ecuación de grado $2, 3$ ó 4 es resoluble por radicales.*

≡

Si E representa al cuerpo raíz de una de estas ecuaciones polinómicas sobre un cuerpo F, entonces $Gal(E/F)$ es un subgrupo de Σ_2, Σ_3 ó Σ_4, todos ellos grupos resolubles. Como todo subgrupo de uno resoluble lo sigue siendo, se tiene que $Gal(E/F)$ es resoluble, conecuentemente E es una extensión radical de F y la ecuación es resoluble por radicales. ♣

Ex. 283 *Comprobar que el cambio $x = X + \frac{p}{3}$ hace que la ecuación cúbica $x^3 - px^2 + qx - r = 0$ se transforme en $X^3 + QX - R = 0$.*

$\equiv$

$$\begin{aligned} 0 &= (X+\frac{p}{3})^3 - p(X+\frac{p}{3})^2 + q(X+\frac{p}{3}) - r \\ &= X^3 + pX^2 + \frac{p^2}{3}X + \frac{p^3}{27} - p(X^2 + \frac{2p}{3}X + \frac{p^2}{9}) + qX + \frac{pq}{3} - r \\ &= X^3 + (q - \frac{p^2}{3})X - (\frac{2p^3}{27} - \frac{pq}{3} + r) \;=\; X^3 + QX - R, \end{aligned}$$

tomando $Q := q - \frac{p^2}{3}$, $R := \frac{2p^3}{27} - \frac{pq}{3} + r$. ♣

Ex. 284 *Deducir las fórmulas de Cardano de la cúbica $x^3 + qx - r = 0$ a partir de la solución dada por*

$$\alpha_1 = \frac{1}{3}(\varepsilon_1 + \varepsilon_2), \quad \alpha_2 = \frac{1}{3}(\rho^2\varepsilon_1 + \rho\varepsilon_2), \quad \alpha_3 = \frac{1}{3}(\rho\varepsilon_1 + \rho^2\varepsilon_2),$$

siendo

$$\rho = \mathrm{e}^{\frac{2\pi\mathrm{i}}{3}}, \quad \varepsilon_1 = \sum_{j=0}^{2} \rho^j (123)^j(\alpha_1), \quad \varepsilon_2 = \sum_{j=0}^{2} \rho^{2j} (123)^j(\alpha_1).$$

$\equiv$

Expliquemos primero cómo se calculan los valores ε_1 y ε_2. Para ello, basta con que indiquemos que (123) representa el ciclo de Σ_3 tal que

$$\begin{aligned} &(123)(\alpha_1) = \alpha_2 \\ &(123)^2(\alpha_1) = (123)(\alpha_2) = \alpha_3. \end{aligned}$$

Por tanto,

$$\begin{aligned} \varepsilon_1 &= \textstyle\sum_{j=0}^{2} \rho^j (123)^j(\alpha_1) \;=\; \alpha_1 + \rho\alpha_2 + \rho^2\alpha_3 \\ \varepsilon_2 &= \textstyle\sum_{j=0}^{2} \rho^{2j} (123)^j(\alpha_1) \;=\; \alpha_1 + \rho^2\alpha_2 + \rho\alpha_3. \end{aligned}$$

Usando el valor auxiliar

$$\Delta := \sqrt{-4q^3 - 27r^2} = \sqrt{2^2 \cdot 3^3 (\frac{-q^3}{27} - \frac{r^2}{4})}$$

puede verse que

$$\varepsilon_1^3 = \frac{27}{2}r - \frac{3\sqrt{-3}}{2}\Delta = \frac{27}{2}r - \frac{3}{2}\sqrt{2^2 \cdot 3^4 (\frac{q^2}{27} + \frac{r^2}{4})} = \frac{27}{2}r - 27\sqrt{\frac{q^3}{27} + \frac{r^2}{4}},$$

de donde

$$\varepsilon_1 = 3\sqrt[3]{\frac{r}{2} - \sqrt{\frac{q^3}{27} + \frac{r^2}{4}}}$$

y que

$$\varepsilon_2 = \frac{-3q}{\varepsilon_1} = \frac{-q}{\sqrt[3]{\frac{r}{2} - \sqrt{\frac{q^3}{27} + \frac{r^2}{4}}}} = 3\sqrt[3]{\frac{r}{2} + \sqrt{\frac{q^3}{27} + \frac{r^2}{4}}}.$$

Así

$$\left.\begin{array}{rcl} \alpha_1 &=& \sqrt[3]{\frac{r}{2}+\sqrt{\frac{q^3}{27}+\frac{r^2}{4}}}+\sqrt[3]{\frac{r}{2}-\sqrt{\frac{q^3}{27}+\frac{r^2}{4}}} \\ \alpha_2 &=& \rho\sqrt[3]{\frac{r}{2}+\sqrt{\frac{q^3}{27}+\frac{r^2}{4}}}+\rho^2\sqrt[3]{\frac{r}{2}-\sqrt{\frac{q^3}{27}+\frac{r^2}{4}}} \\ \alpha_3 &=& \rho^2\sqrt[3]{\frac{r}{2}+\sqrt{\frac{q^3}{27}+\frac{r^2}{4}}}+\rho\sqrt[3]{\frac{r}{2}-\sqrt{\frac{q^3}{27}+\frac{r^2}{4}}} \end{array}\right\} \text{(Fòrmulas de Cardano) } \clubsuit$$

Ex. 285 *Resolver las siguientes ecuaciones cúbicas*

a) $x^3+x+3=0$

b) $x^3-x^2-x+2=0.$

c) $x^3-6x^2+11x-6=0.$

≡

En general, la forma canónica de una cúbica es $x^3-px^2+qx-r=0$. Cuando se tiene que el coeficiente $p=0$ decimos que se trata de una cúbica reducida, entonces se pueden aplicar directamente las fórmulas de Cardano del ejercicio previo. En el caso de que $p\neq 0$, se efectúa el cambio indicado anteriormente para obtener una cúbica reducida.

a) Para resolver $x^3+x+3=0$, como se trata de una cúbica reducida, aplicamos directamente las fórmulas de Cardano

$$\left.\begin{array}{l} p=0 \\ q=1 \\ r=-3 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \Delta^2=-4-243=-247 \\ \varepsilon_1^3=\frac{27}{2}(-3)-\frac{3\sqrt{-3}}{2}\sqrt{-247}=\frac{-1}{2}(81+3\sqrt{741}) \\ \varepsilon_2^3=\frac{-1}{2}(81-3\sqrt{741}), \end{array}\right.$$

de lo que

$$\begin{array}{rcl} \alpha_1 &=& \frac{-1}{3}(\sqrt[3]{\frac{81+3\sqrt{741}}{2}}+\sqrt[3]{\frac{81-3\sqrt{741}}{2}}) \\ \alpha_2 &=& \frac{-1}{3}(\rho\sqrt[3]{\frac{81+3\sqrt{741}}{2}}+\rho^2\sqrt[3]{\frac{81-3\sqrt{741}}{2}}) \\ \alpha_3 &=& \frac{-1}{3}(\rho^2\sqrt[3]{\frac{81+3\sqrt{741}}{2}}+\rho\sqrt[3]{\frac{81-3\sqrt{741}}{2}}). \end{array}$$

b) Para resolver $x^3-x^2-x+2=0$, primero vamos a reducirla

$$\left.\begin{array}{l} p=1 \\ q=-1 \\ r=-2 \end{array}\right\} \overset{(x=X+\frac{p}{3}=X+\frac{1}{2})}{\rightarrow} \left\{\begin{array}{l} Q=q-\frac{p^2}{3}=-1-\frac{1}{3}=\frac{-4}{3} \\ R=\frac{2p^3}{27}-\frac{pq}{3}+r=\frac{2}{27}+\frac{1}{3}-2=\frac{-43}{27} \end{array}\right\} \Rightarrow X^3-\frac{4}{3}X+\frac{43}{27}=0.$$

Ahora aplicamos las fórmulas de Cardano para obtener las soluciones en X

$$\begin{array}{rcl} X_1 &=& \sqrt[3]{\frac{R}{2}+\sqrt{\frac{Q^3}{27}+\frac{R^2}{4}}}+\sqrt[3]{\frac{R}{2}-\sqrt{\frac{Q^3}{27}+\frac{R^2}{4}}} \\ X_2 &=& \rho\sqrt[3]{\frac{R}{2}+\sqrt{\frac{Q^3}{27}+\frac{R^2}{4}}}+\rho^2\sqrt[3]{\frac{R}{2}-\sqrt{\frac{Q^3}{27}+\frac{R^2}{4}}} \\ X_3 &=& \rho^2\sqrt[3]{\frac{R}{2}+\sqrt{\frac{Q^3}{27}+\frac{R^2}{4}}}+\rho\sqrt[3]{\frac{R}{2}-\sqrt{\frac{Q^3}{27}+\frac{R^2}{4}}}, \end{array}$$

de donde

$$X_1 = \tfrac{1}{3}(\sqrt[3]{\tfrac{-43+3\sqrt{177}}{2}} + \sqrt[3]{\tfrac{-43-3\sqrt{177}}{2}})$$

$$X_2 = \tfrac{1}{3}(\rho\sqrt[3]{\tfrac{-43+3\sqrt{177}}{2}} + \rho^2\sqrt[3]{\tfrac{-43-3\sqrt{177}}{2}})$$

$$X_3 = \tfrac{1}{3}(\rho^2\sqrt[3]{\tfrac{-43+3\sqrt{177}}{2}} + \rho\sqrt[3]{\tfrac{-43-3\sqrt{177}}{2}}).$$

Descambiando

$$\begin{aligned}
x_1 &= X_1 + \tfrac{1}{3} = \tfrac{1}{3}(1 + \sqrt[3]{\tfrac{-43+3\sqrt{177}}{2}} + \sqrt[3]{\tfrac{-43-3\sqrt{177}}{2}}) \\
x_2 &= X_2 + \tfrac{1}{3} = \tfrac{1}{3}(1 + \rho\sqrt[3]{\tfrac{-43+3\sqrt{177}}{2}} + \rho^2\sqrt[3]{\tfrac{-43-3\sqrt{177}}{2}}) \\
x_3 &= X_3 + \tfrac{1}{3} = \tfrac{1}{3}(1 + \rho^2\sqrt[3]{\tfrac{-43+3\sqrt{177}}{2}} + \rho\sqrt[3]{\tfrac{-43-3\sqrt{177}}{2}}).
\end{aligned}$$

c) Finalmente resolvemos la ecuación $x^3 - 6x^2 + 11x - 6 = 0$. Primero reducimos

$$\left.\begin{array}{l} p = 6 \\ q = 11 \\ r = 6 \end{array}\right\} \overset{(x=X+\frac{p}{3}=X+2)}{\to} \left\{\begin{array}{l} Q = q - \frac{p^2}{3} = 11 - 12 = -1 \\ R = \frac{2p^3}{27} - \frac{pq}{3} + r = 16 - 22 + 6 = 0 \end{array}\right\} \Rightarrow\ X^3 - X = 0.$$

Aplicamos las fórmulas de Cardano para hallar las raíces para X para comprobar la eficacia del método, ya que dichas raíces son mentalmente calculables

$$\left.\begin{array}{l} Q = -1 \\ R = 0 \end{array}\right\} \Rightarrow \left\{\begin{array}{rcl}
X_1 &=& \sqrt[3]{\frac{R}{2} + \sqrt{\frac{Q^3}{27} + \frac{R^2}{4}}} + \sqrt[3]{\frac{R}{2} - \sqrt{\frac{Q^3}{27} + \frac{R^2}{4}}} = \sqrt[3]{\sqrt{\frac{-1}{27}}} + \sqrt[3]{-\sqrt{\frac{-1}{27}}} = 0 \\
X_2 &=& \rho\sqrt[3]{\frac{R}{2} + \sqrt{\frac{Q^3}{27} + \frac{R^2}{4}}} + \rho^2\sqrt[3]{\frac{R}{2} - \sqrt{\frac{Q^3}{27} + \frac{R^2}{4}}} \\
&=& \rho\sqrt[3]{\sqrt{\frac{-1}{27}}} + \rho^2\sqrt[3]{-\sqrt{\frac{-1}{27}}} = \sqrt[6]{\frac{-1}{27}}(\rho - \rho^2) = \frac{\sqrt[6]{-1}}{\sqrt{3}}\mathbf{i}\sqrt{3} = -1 \\
X_3 &=& \rho^2\sqrt[3]{\frac{R}{2} + \sqrt{\frac{Q^3}{27} + \frac{R^2}{4}}} + \rho\sqrt[3]{\frac{R}{2} - \sqrt{\frac{Q^3}{27} + \frac{R^2}{4}}} \\
&=& \rho^2\sqrt[3]{\sqrt{\frac{-1}{27}}} + \rho\sqrt[3]{-\sqrt{\frac{-1}{27}}} = \sqrt[6]{\frac{-1}{27}}(\rho^2 - \rho) = \frac{\sqrt[6]{-1}}{\sqrt{3}}(-\mathbf{i}\sqrt{3}) = 1,
\end{array}\right.$$

de lo que

$$\left\{\begin{array}{l} x_1 = X_1 + 2 = 2 \\ x_2 = X_2 + 2 = 1 \\ x_3 = X_3 + 2 = 3. \ \clubsuit \end{array}\right.$$

Nota 32 Como todo el mundo habrá observado, la última ecuación es un ejemplo sencillo para ilustrar la Regla de Ruffini (Paolo), también conocida en el mundo anglosajón como Horner's rule

Ex. 286 *Encontrar ecuaciones cúbicas sobre* $\mathbf{Q}$ *cuyos grupos de Galois sean de orden* 1, 2, 3 *y* 6.

$\equiv$

1) La cúbica $x^3 - 3x^2 + 3x - 1 = 0$ tiene a $x = 1$ como única raíz, por lo que, al descomponerse el polinomio $x^3 - 3x^2 + 3x - 1 = (x-1)^3 \in \mathbf{Q}[x]$ en $\mathbf{Q}$, se tiene que su cuerpo raíz es $E = \mathbf{Q}$. Claramente $Gal(E/\mathbf{Q}) = \{Id_{\mathbf{Q}}\}$.

2) La ecuación $x(x^2 - 2) = 0$ tiene como cuerpo raíz a $E := \mathbf{Q}(\sqrt{2})$. Ya sabemos que $[E : \mathbf{Q}] = 2$, con lo que $Gal(E/\mathbf{Q})$ es de orden 2. De hecho, $Gal(\mathbf{Q}(\sqrt{2}/\mathbf{Q}) = \{Id_{\mathbf{Q}(\sqrt{2})}, \varphi\}$, donde

$$\varphi(a + b\sqrt{2}) \quad = \quad a - b\sqrt{2}, \qquad a, b \in \mathbf{Q}.$$

Los siguientes resultados auxiliares van a ser de importancia para los dos apartados restantes.

Lema 11 *Sea $x^3 - px^2 + qx - r \in \mathbf{Q}[x]$ irreducible sobre $\mathbf{Q}$. Sean α_1, α_2 y α_3 las raíces de dicho polinomio y sea $\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$. Si $\Delta \in \mathbf{Q}$, entonces el cuerpo raíz del polinomio es $\mathbf{Q}(\alpha_1)$.*

$\equiv$

Como

$$\left.\begin{array}{l} \alpha_1 + \alpha_2 + \alpha_3 = p \in \mathbf{Q} \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = q \in \mathbf{Q} \\ \alpha_1\alpha_2\alpha_3 = r \in \mathbf{Q}, \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \alpha_2 + \alpha_3 \in \mathbf{Q}(\alpha_1) \\ \alpha_2\alpha_3 \in \mathbf{Q}(\alpha_1) \end{array}\right\} \Rightarrow (x-\alpha_2)(x-\alpha_3) \in \mathbf{Q}(\alpha_1)[x],$$

así, para $x = \alpha_1$, se tiene que $(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) \in \mathbf{Q}(\alpha_1)$. Consecuentemente, al suponer que $\Delta \in \mathbf{Q}$, tenemos

$$\alpha_2 - \alpha_3 \quad = \quad \frac{\Delta}{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)} \in \mathbf{Q}(\alpha_1).$$

Entonces

$$\left.\begin{array}{l} \alpha_2 + \alpha_3 \in \mathbf{Q}(\alpha_1) \\ \alpha_2 - \alpha_3 \in \mathbf{Q}(\alpha_1) \end{array}\right\} \Rightarrow \alpha_2,\ \alpha_3 \in \mathbf{Q}(\alpha_1) \Rightarrow \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbf{Q}(\alpha_1). \bullet$$

Corolario 1 *Sea $x^3 - px^2 + qx - r \in \mathbf{Q}[x]$ irreducible sobre $\mathbf{Q}$. Con la terminología del lema previo, supongamos que $\Delta \in \mathbf{Q}$. Si E es el cuerpo raíz del polinomio, entonces $Gal(E/\mathbf{Q})$ es el grupo alternado de $\alpha_1, \alpha_2, \alpha_3$.*

$\equiv$

Ya sabemos, del lema, que $E = \mathbf{Q}(\alpha_1)$. Por tanto, $o(Gal(E/\mathbf{Q})) = [E : \mathbf{Q}] = 3$. También sabemos que $Gal(E/\mathbf{Q})$ es (isomorfo a) un subgrupo del grupo simétrico del conjunto $\{\alpha_1, \alpha_2, \alpha_3\}$; como $A_3 = \langle\ (123)\ \rangle$ es el único subgrupo de Σ_3 de orden 3, queda claro que $Gal(E/\mathbf{Q})$ es isomorfo a A_3. $\bullet$

3) La ecuación $x^3 - 3x + 1 = 0$ cumple que

$$\left.\begin{array}{l} p = 0 \\ q = -3 \\ r = -1 \end{array}\right\} \Rightarrow \Delta^2 = -4(-27) - 27 = 81 \Rightarrow \Delta \in \mathbf{Q}.$$

Aplicando el corolario anterior, el orden del grupo $Gal(E/\mathbf{Q})$ es 3. De hecho, si $\alpha_1, \alpha_2, \alpha_3$ son las raíces,

$$Gal(E/\mathbf{Q}) \;=\; Gal(\mathbf{Q}(\alpha_1)/\mathbf{Q}) \;=\; \{\; Id_{\mathbf{Q}(\alpha_1)}, (\alpha_1\alpha_2\alpha_3), (\alpha_1\alpha_3\alpha_2) \;\}.$$

4) La ecuación $x^3 - 2 = 0$ tiene un grupo de Galois de orden 6, ya que vimos en ejercicios anteriores que su cuerpo raíz es $E = \mathbf{Q}(\sqrt[3]{2}, \mathrm{e}^{\frac{2\pi\mathbf{i}}{3}})$, de lo que

$$o(Gal(E/\mathbf{Q}) \;=\; [\mathbf{Q}(\sqrt[3]{2}, \mathrm{e}^{\frac{2\pi\mathbf{i}}{3}}) : \mathbf{Q}] \;=\; 6. \;\clubsuit$$

Ex. 287 *Dada la cúbica $x^3 - px^2 + qx - r = 0$ sobre $\mathbf{Q}$, con raíces $\alpha_1, \alpha_2, \alpha_3$.*
Si $\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$, demostrar que
a) $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$ si y sólo si $\Delta^2 \geq 0$.
b) Exactamente una de las raíces es real si y sólo si $\Delta^2 < 0$.

$\equiv$

Obsérvese antes de empezar que, puesto que todo polinomio de grado impar de coeficientes reales admite al menos una raíz real (una consecuencia elemental del teorema de Bolzano), es inmediato que las dos sentencias de ambos apartados son equjivalentes, por lo que basta con demostrar la primera.
a)
[$\Rightarrow$] Supongamos que $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$. Entonces, al tratarse de números reales (donde vale la regla de los signos), se tiene que

$$\Delta^2 \;=\; (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 \;\geq\; 0.$$

[$\Leftarrow$] Si $\Delta^2 \geq 0$, distinguimos dos casos:
Uno. $\Delta = 0$. Entonces hay dos raíces iguales. Sean por comodidad $\alpha_1 = \alpha_2$. Como la cúbica siempre tiene al menos una raíz real, las otras dos raíces, en caso de ser complejas puras, serían conjugadas. Ello obliga a que $\alpha_1 = \alpha_2, \alpha_3 \in \mathbf{R}$.
Dos. $\Delta^2 > 0$. Ahora, suponiendo que sólo hay una raíz real, se tendría (por ejemplo)

$$\alpha_1 \in \mathbf{R}, \quad \alpha_2 \;=\; a + b\mathbf{i}, \quad \alpha_3 \;=\; a - b\mathbf{i}, \quad a, b \in \mathbf{R},\; b \neq 0.$$

Pero entonces

$$\Delta^2 \;=\; (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 \;=\; [(\alpha_1 - a) - b\mathbf{i}]^2[(\alpha_1 - a) + b\mathbf{i}]^2(2b\mathbf{i})^2$$

$$=\; -4b^2[(\alpha_1 - a)^2 + b^2]^2 \;<\; 0,$$

lo que es absurdo. $\clubsuit$

Ex. 288 *Sea $f(x)$ un polinomio de tercer grado irreducible sobre $\mathbf{Q}$. Demostrar que el cuerpo raíz de $f(x)$ sobre $\mathbf{Q}$ es $\mathbf{Q}(\alpha, \Delta)$, siendo α una de sus raíces y Δ el discriminante utilizado en ejercicios anteriores.*

$\equiv$

Si α, β, γ son las tres raíces de $f(x) \in \mathbf{Q}[x]$, entonces

$$f(x) = a(x-\alpha)(x-\beta)(x-\gamma), \quad a \in \mathbf{Q},$$

$$\Delta = (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha).$$

Como el cuerpo raíz de $f(x)$ sobre $\mathbf{Q}$ es claramente $E := \mathbf{Q}(\alpha, \beta, \gamma)$, todo se reduce a ver que $\beta, \gamma \in \mathbf{Q}(\alpha, \Delta)$. Observemos que

$$\left.\begin{array}{l} f(x) = a(x-\alpha)(x-\beta)(x-\gamma) \in \mathbf{Q}[x] \subset \mathbf{Q}(\alpha,\Delta)[x] \\ a(x-\alpha) \in \mathbf{Q}(\alpha,\Delta)[x] \end{array}\right\} \Rightarrow (x-\beta)(x-\gamma) \in \mathbf{Q}(\alpha,\Delta)[x].$$

Ello implica que $\beta+\gamma, \beta\gamma \in \mathbf{Q}(\alpha, \Delta)$. Además, como, para $x = \alpha$, $(\alpha-\beta)(\alpha-\gamma) \in \mathbf{Q}(\alpha, \Delta)$, se sigue que

$$\left.\begin{array}{l} \beta-\gamma = \frac{\Delta}{(\alpha-\beta)(\gamma-\alpha)} \in \mathbf{Q}(\alpha,\Delta) \\ \beta+\gamma \in \mathbf{Q}(\alpha,\Delta) \end{array}\right\} \Rightarrow \beta, \gamma \in \mathbf{Q}(\alpha, \Delta). \clubsuit$$

Ex. 289 *Demostrar que una ecuación cúbica irreducible sobre* $\mathbf{Q}$ *con tres raíces reales no puede resolverse sólo por radicales reales.*

$\equiv$

[Esta resolución es una adaptación del Teorema 22 de [1, pág. 484]]

Sea $f(x) = x^3 - px^2 + qx - r \in \mathbf{Q}[x]$ irreducible sobre $\mathbf{Q}$ tal que sus raíces $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$. Si E es el cuerpo raíz de $f(x)$ sobre $\mathbf{Q}$, sabemos del ejercicio previo que $E = \mathbf{Q}(\alpha_1, \Delta)$, donde como siempre $\Delta = (\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)$. También de un ejercicio anterior sabemos que, como $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$, entonces $\Delta^2 \geq 0$. Consecuentemente, $E = \mathbf{Q}(\alpha_1, \Delta) \subset \mathbf{R}$. Supongamos que la raíz α_1 puede ser obtenida mediante radicales reales. Eso significa lo siguiente:

Existen $\sqrt[r_1]{a_1}, \sqrt[r_2]{a_2}, ..., \sqrt[r_n]{a_n} \in \mathbf{R}$, con $r_1, r_2, ..., r_n$ primos, tales que $\alpha_1 \in \mathbf{Q}(\sqrt[r_1]{a_1}, \sqrt[r_2]{a_2}, ..., \sqrt[r_n]{a_n})$.

Llamando $K_1 := \mathbf{Q}(\Delta)$, $K_2 := K_1(\sqrt[r_1]{a_1}), ..., K_{n+1} := K_n(\sqrt[r_n]{a_n})$, obtenemos una torre de cuerpos

$$K_1 \subset K_2 \subset ... \subset K_{n+1} = \mathbf{Q}(\Delta, \sqrt[r_1]{a_1}, \sqrt[r_2]{a_2}, ..., \sqrt[r_n]{a_n}) \subset \mathbf{R}.$$

Para cada $i = 1, 2, ..., n$, $[K_{i+1} : K_i] = r_i$, ya que el polinomio $x^{r_i} - a_i$ es irreducible sobre K_i, al ser r_i primo. Como $E = \mathbf{Q}(\Delta, \alpha_1) \subset K_{n+1}$, existe un $j \in \{1, 2, ..., n\}$ tal que $\alpha_1, \alpha_2, \alpha_3 \notin K_j$ y alguna de las raíces, por ejemplo, $\alpha_1 \in K_{j+1}$. Entonces $[K_j(\alpha_1) : K_j] = 3$, ya que $f(x) \in \mathbf{Q}[x] \subset K_j[x]$ y $f(x)$ es irreducible sobre K_j, pues $\alpha_1, \alpha_2, \alpha_3 \notin K_j$. Pero

$$r_j = [K_{j+1} : K_j] = [K_{j+1} : K_j(\alpha_1)] \cdot [K_j(\alpha_1) : K_j] = 3 \cdot [K_{j+1} : K_j(\alpha_1)]$$

$$\Rightarrow 3 \mid r_j \overset{(r_j \text{ primo})}{\Rightarrow} r_j = 3.$$

Por tanto, $K_{j+1} = K_j(\sqrt[3]{a_j})$. Ello implica que $K_{j+1} \supset \mathbf{Q}(\Delta, \sqrt[3]{a_j})$, que es el cuerpo raíz de la cúbica $x^3 - a_j = 0$. Consecuentemente, $e^{\frac{2\pi i}{3}} \sqrt[3]{a_j} \in K_{j+1}$, de donde se deduce que $e^{\frac{2\pi i}{3}} \in K_{j+1}$. Absurdo, pues $K_{j+1} \subset \mathbf{R}$. $\clubsuit$

Ex. 290 *Construir un polinomio de grado 7 que sea irreducible sobre* $\mathbf{Q}$ *y no resoluble por radicales.*

≡

La construcción de semejante polinomio es la siguiente:

Necesitamos un polinomio de séptimo grado con coeficentes en $\mathbf{Z}$ (es equivalente a que sea de $\mathbf{Q}[x]$) que sea irreducible sobre $\mathbf{Q}$ y cuyo grupo de Galois sea Σ_7, que al no ser resoluble nos garantiza que la correspondiente ecuación polinómica no es resoluble por radicales. Para ello, como por ser irreducible $Gal(E/\mathbf{Q})$, siendo E el cuerpo raíz del polinomio, es transitivo, precisamos que tenga cinco raíces reales y dos complejas (evidentemente conjugadas). Ello implica que el polinomio, vamos a llamarle $f(x)$, ha de tener 4 extremos relativos (dos máximos y dos mínimos). Supongamos que dichos extremos están en $, -2-1, 1, 2$. Como estos valores han de ser raíces de $f'(x)$, entonces la forma del polinomio derivada es

$$f'(x) = a\,(x+2)(x+1)(x-1)(x-2)g(x) = a(x^2-4)(x^2-1)g(x) = a(x^4-5x^2+4)g(x),$$

con $a \in \mathbf{Q}$, $g(x) \in \mathbf{Q}[x]$ polinomio de segundo grado con raíces complejas. Así pues, tomando (por ejemplo)

$$f'(x) = a\,(x^4 - 5x^2 + 4)(x^2 + 1) = a\,(x^6 - 4x^4 - x^2 + 4),$$

integrando

$$f(x) = a\,(\frac{x^7}{7} - \frac{4}{5}x^5 - \frac{x^3}{3} + 4x) + C.$$

Sea por tanto, multiplicando por 105 y tomando $C := 7$,

$$f(x) = 15x^7 - 84x^5 - 35x^3 + 420x + 7.$$

Aplicando el criterio de Esisenstein se vé que $f(x)$ es irreducible sobre $\mathbf{Q}$. Consecuentemente, $Gal(E/\mathbf{Q})$ es un subgrupo transitivo de Σ_7. Ahora bien, como

$$f'(x) = 105(x+2)(x+1)(x-1)(x-2)(x^2+1),$$

los cambios de signo en $f(x)$ nos indican que tiene 5 raíces reales en los intervalos

$$]-4,-2[\,\cup\,]-2,-1[\,\cup\,]-1,1[\,\cup\,]1,2[\,\cup\,]2,4[.$$

Sean $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$ dichas raíces reales y sean $\alpha_6, \alpha_7 \in \mathbf{C}$, $\overline{\alpha_6} = \alpha_7$. Entonces el automorfismo

$$\begin{array}{rccc} \Phi & : & E & \longrightarrow & E \\ & & z & \to & \Phi(z) = \overline{z} \end{array}$$

cumple que $\Phi(\alpha_6) = \alpha_7$, $\Phi(\alpha_7) = \alpha_6$, por lo que, como $\Phi \in Gal(E/\mathbf{Q})$, se tiene que Φ equivale a la trasposición (α_6, α_7), con lo que $Gal(E/\mathbf{Q}) = \Sigma_7$, como queríamos. ♣

Ex. 291 *Demostrar que para todo primo* $p > 3$ *existe un polinomio* $f(x)$ *de grado* p *que es irreducible sobre* $\mathbf{Q}$ *y que no es resoluble por radicales.*

$\equiv$

La idea consiste en usar el procedimiento del ejercicio previo para este caso más general. Así, consideramos el polinomio

$$(x+\frac{p-3}{2})(x+\frac{p-5}{2})...(x+1)(x-1)...(x-\frac{p-5}{2})(x-\frac{p-3}{2})(x^2+1).$$

Este polinomio tiene grado $p-1$, ya que consta de $p-3$ factores lineales y otro factor de segundo grado. Integrando obtenemos un polinomio de grado p que llamamos $g(x)$. Es más, como $g'(x)$ es un polinomio "bicuadrado", ya que sus raíces reales son pares de números opuestos, la forma de este polinomio es

$$g(x) = \frac{1}{p}x^p + c_1x^{p-2} + c_2x^{p-4} + ... + c_{\frac{p-1}{2}}x.$$

Tomando $k := p(p-2)\cdot(p-4)\cdot ...\cdot 1$ y definiendo $f(x) := k\cdot g(x)+p$ obtenemos un polinomio $f(x)\in \mathbf{Q}[x]$ tal que, como $p \mid k$, $p^2 \not| k$, el criterio de Eisenstein no dice que $f(x)$ es irreducible sobre $\mathbf{Q}$. Por tanto, $Gal(E/\mathbf{Q})$ es un subgrupo transitivo de Σ_p, siendo E el cuerpo raíz de $f(x)$. Observando que $f'(x) = kg'(x)$ tiene $p-3$ raíces reales en

$$\pm\frac{p-3}{2},\ \pm\frac{p-5}{2},\ ...\ \pm\frac{p-(2\frac{p-3}{2}+1)}{2} = \pm 1,$$

podemos afirmar, a partir de que los puntos anteriores son extremos relativos estrictos de $f(x)$, que $f(x)$ tiene $p-2$ raíces reales distintas $\alpha_1,\alpha_2,...,\alpha_{p-2}$ localizadas en los intervalos abiertos determinados por los ceros de $f'(x)$. Además, $f(x)$ tiene dos raíces complejas conjugadas α_{p-1},α_p. Por tanto, el automorfismo de E definido por $\Phi(z) := \overline{z}$, que pertenece al grupo de Galois $Gal(E/\mathbf{Q})$, es equivalente a la transposición $(\alpha_{p-1},\alpha_p)\in \Sigma_p$. Ello implica que $Gal(E/\mathbf{Q}) = \Sigma_p$ que, al ser $p>3$, no es resoluble. ♣

Capítulo 4

Teoría de anillos

4.1. Generalidades y ejemplos de anillos

Ex. 292 *Indicar cuales de las siguientes estructuras algebraicas son anillos:*

a) $(\mathbf{Z}, +, \cdot)$.
b) $(2\mathbf{Z}, +, \cdot)$.
c) $(\mathbf{Z}_n, +, \cdot)$.
d) $(\mathbf{Q}, +, \cdot)$.
e) $(\mathbf{Q}^+, +, \cdot)$.
f) $(\mathbf{R}, +, \cdot)$.
g) $(\mathbf{C}, +, \cdot)$.
h) $(Im, +, \cdot)$.
i) $(\mathbf{Z}(\sqrt{-3}), +, \cdot)$.
j) $(F[x], +, \cdot)$, *F un cuerpo.*
k) $(\mathbf{Z}[x], +, \cdot)$.
l) $(\mathbf{Z}_{prim}[x], +, \cdot)$, *donde* $\mathbf{Z}_{prim}[x]$ *es el conjunto de polinomios primitivos.*
m) $(M_{(2\times 2)}, +, \cdot)$.
n) $(C(\mathbf{R}), +, \cdot)$.
o) $(\mathbf{R}_\infty[x], +, \cdot)$.
p) $(\mathbf{Q}_p, +, \cdot)$, *siendo, para p primo,* $\mathbf{Q}_p = \{\frac{a}{b} \in \mathbf{Q} \ : \ mcd(a,b) = 1, \ p \not| \ b \ \}$.
q) $(2^X, \cup, \cap)$.
r) $(2^X, \diamond, \cap)$.
s) $(End(G), +, \circ)$, *donde $End(G)$ representa al conjunto de los endomorfismos del grupo abeliano $(G, +)$.*
t) $(\mathbf{Z}, \oplus, \otimes)$, *siendo* $a \oplus b := \ a + b + 1$, $a \otimes b := \ ab + a + b$.

$\equiv$

Antes, recordemos que por anillo se entiende una estructura algebraica bioperativa $(A, +, \cdot)$ que ha de cumplir las siguientes condiciones

1) $(A, +)$ ha de ser un grupo abeliano.
2) $(A, \cdot)$ ha de ser un semigrupo, i.e., $\cdot$ ha de ser estable y asociativa.

3) $\cdot$ ha de ser distributiva por la izquierda y por la derecha respecto de $+$, es decir

$$\forall a,b,c \in A, \quad \begin{cases} a\cdot(b+c) &= a\cdot b + a\cdot c \\ (b+c)\cdot a &= b\cdot a + c\cdot a. \end{cases}$$

Cuando $(A,+,\cdot)$ cumple, además de las condiciones de anillo,

$\cdot$ tiene neutro, i.e. $\exists 1 \in A$ tal que $\forall a \in A,\ a\cdot 1 = 1\cdot a = a$
$\rightarrow$ $(A,+,\cdot)$ es un anillo unitario

$\cdot$ es conmutativa $\rightarrow$ $(A,+,\cdot)$ es un anillo conmutativo

$$a,b \in A \ / \ a\cdot b = 0 \ \rightarrow \ \left\{ \begin{array}{c} a=0 \\ \acute{o} \\ b=0 \end{array} \right\} \rightarrow \ (A,+,\cdot) \text{ es un anillo integro}$$

Si$(A,+,\cdot)$ es unitario conmutativo e integro, se llama dominio de integridad.

Cuando un anillo $(A,+,\cdot)$ no es íntegro, entonces existen al menos dos elementos $a,b \in A$ tales que $a \neq 0$, $b \neq 0$ y $ab = 0$; a estos elementos se les llama divisores de cero. Así, un anillo es íntegro siempre que no admite divisores de cero. Conviene observar que un cuerpo es un anillo, de hecho, un dominio de integridad.

a) $(\mathbf{Z}+,\cdot)$ es dominio de integridad.

b) $(2\mathbf{Z},+,\cdot)$ es un subanillo de $(\mathbf{Z},+,\cdot)$. Como cabe esperar, un subanilo B de un anillo $(A,+,\cdot)$ es un subconjunto $B \subset A$ tal que, al ser dotado de las operaciones de A restringidas a B, cumple todas las condiciones de modo que $(B,+,\cdot)$ resulta un anillo. Como suele pasar con las subestructuras algebraicas hay una condición caracterizadora de cuándo un subconjunto es un subanillo de un anillo dado: En un anillo $(A,+,\cdot)$

$$B \ \subset A \ \text{ es un subanillo } \Leftrightarrow \ \forall a,b \in B, \ \begin{cases} a-b \in B \\ a\cdot b \in B. \end{cases}$$

Por tanto, $2\mathbf{Z}$ es también un anillo, aunque no es unitario, pues $1 \notin 2\mathbf{Z}$.

c) $\mathbf{Z}_n$ es un anillo unitario y conmutativo. Notar que

$$\mathbf{Z}_n \text{ es cuerpo } \Leftrightarrow \ \mathbf{Z}_n \text{ es integro } \Leftrightarrow \ \text{ n primo.}$$

d) $\mathbf{Q}$ es un cuerpo.

e) $\mathbf{Q}^+$ no es anillo, ya que $\mathbf{Q}^*,+)$ no es un grupo (no tiene opuestos).

f) $\mathbf{R}$ es un cuerpo.

g)) $\mathbf{C}$ es un cuerpo.

h) $Im = \{\ k\mathbf{i} \ : \ k \in \mathbf{R}\ \}$ no es anillo puesto que el producto no es estable en Im:

$$\text{Si } k,r \in \mathbf{R}\setminus\{0\}, \ \ (k\mathbf{i}\cdot(r\mathbf{i}) \ = \ kr\mathbf{i}^2 \ = \ -kr \ \notin \ Im.$$

i)) $\mathbf{Z}(\sqrt{-3}$ es un subanillo (dominio de integridad, por tanto) de $\mathbf{C}$: Si $a+b\sqrt{-3}, c+d\sqrt{-3} \in \mathbf{Z}(\sqrt{-3})$

$$(a+b\sqrt{-3})-(c+d\sqrt{-3}) = (a-c)+(b-d)\sqrt{-3} \in \mathbf{Z}(\sqrt{-3})$$
$$(a+b\sqrt{-3})\cdot(c+d\sqrt{-3}) = (ac-3bd)+(ad+bc)\sqrt{-3} \in \mathbf{Z}(\sqrt{-3}).$$

j)) $F[x]$ es un dominio de integridad siempre que F sea cuerpo. Se demuestra de forma similar a que el conjunto de polinomios $\mathbf{Q}[x]$ es un dominio de integridad.
k)) $\mathbf{Z}[x]$ es un dominio de integridad. Se trata de un subanillo de $\mathbf{Q}[x]$, por tanto hereda sus mismas propiedades en lo referente a la estructura de anillo.
l) $\mathbf{Z}_{prim}[x]$ es el conjunto de todos los polinomios primitivos con coeficientes en $\mathbf{Z}$. Recordemos que $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbf{Z}[x]$ es un polinomio primitivo siempre que cumple que $mcd(a_0, a_1, ..., a_n) = 1$. Es evidente que $\mathbf{Z}_{prim}[x]$ no es anillo, ya que $0 \notin \mathbf{Z}_{prim}[x]$.
m) $M_{(2\times 2)}$ es el conjunto de todas las matrices reales de dimensiones (2×2). Veamos que es un anillo unitario, pero no conmutativo y no íntegro. Verificar las condiciones de anillo para $(M_{(2\times 2)}, +, \cdot)$ es mecánico. Se trata de un anillo unitario, ya que su unidad es $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Los siguientes ejemplos demuestran que este anillo ni es conmutativo ni íntegro.

$$A := \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, \quad B := \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} \left\{ \begin{array}{l} AB = \begin{pmatrix} 5 & 0 \\ 0 & 0 \end{pmatrix} \\ \\ BA = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \end{array} \right\} \Rightarrow AB \neq BA.$$

Por (0) indicamos la matriz-cero (2×2), i.e., la que todos sus coeficientes son cero.

$$\begin{aligned} A &:= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq (0) \\ B &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq (0) \\ AB &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = (0). \end{aligned}$$

n) $C(\mathbf{R})$ es el conjunto de todas las funciones $f : \mathbf{R} \to \mathbf{R}$ que son continuas. Veamos que es un anillo unitario conmutativo, pero no íntegro. De nuevo, comprobar que se trata de un anillo es mecánico. Es unitario ya que su unidad es la función $\mathbf{1}(x) = 1$, $\forall x \in \mathbf{R}$, que es claramente continua (una recta horizontal). Además, la estructura es conmutativa respecto del producto ordinario de funciones. Para ver que no es una estructura íntegra buscamos dos funciones $f \neq 0$, $g \neq 0$ de $\mathbf{C}(\mathbf{R})$ tales que $fg = 0$, es decir, dos divisores de cero en $C(\mathbf{R})$. Basta tomar (hacer un dibujo es ilustrativo)

$$\left. \begin{array}{l} f(x) = \left\{ \begin{array}{ll} 0, & x \in]-\infty, 0], \\ x, & x \in]0, +\infty[\end{array} \right. \\ \\ g(x) = \left\{ \begin{array}{ll} x, & x \in]-\infty, 0], \\ 0, & x \in]0, +\infty[\end{array} \right. \end{array} \right\} \Rightarrow f \neq 0, \ g \neq 0, \ fg = 0.$$

o) $\mathbf{R}_\infty[x]$ es el conjunto de todas las series de potencias de coeficientes reales, i.e.

$$\mathbf{R}_\infty[x] = \{ \sum_{n=0}^{\infty} a_n x^n : a_n \in \mathbf{R}, \ n = 0, 1, ... \}.$$

Comprobar que es un anillo es mecánico..., quizás convenga explicitarlo

$$(\sum_{n=0}^{\infty} a_n x^n) + (\sum_{n=0}^{\infty} b_n x^n) = \sum_{n=0}^{\infty} (a_n + b_n) x^n; \quad (\sum_{n=0}^{\infty} a_n x^n) \cdot (\sum_{n=0}^{\infty} b_n x^n)$$

$$= \sum_{n=0}^{\infty} c_n x^n, \text{ con } c_n = \sum_{k=0}^{n} a_{n-k} b_k.$$

Este anillo es unitario: $1 \in \mathbf{R} \subset \mathbf{R}[x] \subset \mathbf{R}_\infty[x]$. Es claramente conmutativo y se puede demostrar de manera análoga a como se hace para polinomios que no tiene divisores de cero. Así pues $\mathbf{R}_\infty[x]$ es un dominio de integridad.

p) Para p primo, $\mathbf{Q}_p = \{ \frac{a}{b} \in \mathbf{Q} : mcd(a,b) = 1, \ p \not| \ b\}$. Veamos que $\mathbf{Q}_p$ es un subanillo de $\mathbf{Q}$: Si $\frac{a}{b}, \frac{c}{d} \in \mathbf{Q}_p$, entonces

$$\begin{cases} \frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd} \\ \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}; \end{cases}$$

suponiendo que estas fracciones son ya irreducibles (si no, se reducen y punto), como $p \not| \ b$, $p \not| \ d$, se tiene que $p \not| \ bd$, i.e., $\frac{ad-bc}{bd}, \frac{ac}{bd} \in \mathbf{Q}_p$. Como $\mathbf{Q} \subset \mathbf{Q}_p$, tenemos que $\mathbf{Q}_p$ es unitario y, como además es conmutativo e íntegro, concluimos que es dominio de integridad.

q) Dado un conjunto X, 2^X es la familia de las partes de X. $(2^X, \cup, \cap)$ no es anillo. Para verlo, basta con demostrar que la estructura monooperativa $(2^X, \cup)$ nisiquiera es grupo ya que, aunque hay estabilidad, asociatividad y neutro (el $\emptyset$), en general todo elemento de 2^X no tiene porqué admitir simétrico: Dado $A \in 2^X$, si existiese $B \in 2^X$ tal que $A \cup B = \emptyset$, ello obligaría a que $A = B = \emptyset$.

r) $(2^X, \diamond, \cap)$ sí que es anillo. Vamos verlo despacio.

$$(2^X, \diamond) \begin{cases} \text{Estable}: \ A \diamond B \in 2^X \\ \text{Asociativa}: \begin{cases} (A \diamond B) \diamond C \\ = (A \setminus B \setminus C) \cup (B \setminus A \setminus C) \cup (C \setminus A \setminus B) \cup (A \cap B \cap C) \\ \\ A \diamond (B \diamond C) \\ = (A \setminus B \setminus C) \cup (B \setminus A \setminus C) \cup (C \setminus A \setminus B) \cup (A \cap B \cap C) \end{cases} \\ \text{Neutro}: \ \emptyset \diamond A = A \diamond \emptyset = A \\ \text{Simétricos}: \ A \diamond A = \emptyset \\ \text{Conmutativa}: \ A \diamond B = (A \cup B) \setminus (A \cap B) = B \diamond A \end{cases}$$

$$\cap \begin{cases} \text{Estable}: \ A \cap B \in 2^X \\ \text{Asociativa}: \ (A \cap B) \cap C = A \cap (B \cap C) \\ \text{Distributiva}: \ A \cap (B \diamond C) = [(A \cap B) \setminus C] \cup [(A \cap C) \setminus B] = (A \cap B) \diamond (A \cap C) \\ \text{Conmutativa}: \ A \cap B = B \cap A \\ \text{Unidad}: \ A \cap X = X \cap A = A. \end{cases}$$

Resumiendo, $2^X, \diamond, \cap)$ es una anillo unitario conmutativo, pero en general no es íntegro: Si X tiene más de 1 elemento, entonces existe $A \subset X, \emptyset \neq A \neq X$. Como $A \cap (X \setminus A) = \emptyset$, se tiene que A y $X \setminus A$ son divisores de cero.

s) Dado un grupo abelinao $(G,+)$, sea $End(G)$ el conjunto de los endomorfismos de G, i.e. sus elementos son homomorfismos del grupo G en sí mismo. Definiendo la suma en $End(G)$ de manera natural como

$$\forall f,g \in End(G), \quad (f+g)(x) = f(x)+g(x), \quad x \in G,$$

es inmediato comprobar que $(End(G),+)$ tiene estructura de grupo abeliano. Si 0 es el neutro de G, representamos por $\mathbf{0}$ al neutro de $(End(G),+)$, siendo $\mathbf{0}(x)=0$, para todo $x \in G$. La segunda operación con que vamos a dotar a $End(G)$ va a ser la composición de aplicaciones $\circ$.

Como la composición de homomorfismos de grupos es otro homomorfismo, se tiene que $\circ$ es estable en $End(G)$. Es obviamente asociativa. También es distributiva (a derecha e izquierda) respecto de la suma recién definida: $\forall f,g,h \in End(G)$, $\forall x \in G$,

$$\begin{cases} [f\circ(g+h)](x) = f[(g+h)(x)] = f[g(x)+h(x)] = f[g(x)]+f[h(x)] \\ = (f\circ g)(x)+(f\circ h)(x) \\ \\ [(g+h)\circ f](x) = (g+h)[f(x)] = g[f(x)]+h[f(x)] \\ = (g\circ f)(x)+(h\circ f)(x). \end{cases}$$

Como también tiene elemento unidad (Id_G), tenemos que $(End(G),+,\circ)$ es un anillo unitario, pero no conmutativo ni íntegro. Como contraejemplo de la no-conmutatividad, y también de la no-integridad, tómese: En $G := \mathbf{Z}^2$, consideramos los endomorfismos $f,g,h: \mathbf{Z}^2 \to \mathbf{Z}^2$ dados por

$$\left.\begin{array}{l} f(x,y) := (x,0) \\ g(x,y) := (y,x) \end{array}\right\} \Rightarrow \left\{\begin{array}{l} (f\circ g)(x,y) = f(y,x) = (y,0) \\ (g\circ f)(x,y) = f(x,0) = (0,x) \end{array}\right\} \Rightarrow f\circ g \neq g\circ f$$
$$h(x,y) := (0,y) \Rightarrow (f\circ h)(x,y) = f(0,y) = (0,0) \Rightarrow f\circ h = 0.$$

t) La última estructura es la más rara de todas y, en opinión de este resolvedor, la menos útil (todas las anteriores tienen gran importancia y surgieron promovidas por problemas matemáticos naturales). En $\mathbf{Z}$ se consideran las operaciones

$$\forall a,b \in \mathbf{Z} \quad \begin{cases} a\oplus b = a+b+1 \\ a\otimes b = ab+a+b. \end{cases}$$

Repasemos una por una las condiciones de anillo.
Para $(\mathbf{Z},\oplus)$:
Estable: Evidente.
Asociativa:

$$(a\oplus b)\oplus c = (a+b+1)\oplus c = (a+b+1)+c+1 = a+(b+c+1)+1$$
$$= a+(b\oplus c)+1 = a\oplus(b\oplus c).$$

Neutro: $\forall a \in \mathbf{Z}$, $a\oplus(-1) = (-1)\oplus a = a$.

Simétricos: $\forall a \in \mathbf{Z}, \quad a \oplus (-a-2) = (-a-2) \oplus a = -1.$
Conmutativa: Evidente.
Para $(\mathbf{Z}, \otimes)$:
Estable: Evidente.
Asociativa:

$$(a \otimes b) \otimes c \;=\; (ab+a+b) \otimes c \;=\; (ab+a+b)c + (ab+a+b) + c$$

$$= abc + ab + ac + bc + a + b + c = a \otimes (b \otimes c).$$

Distributivas: Como veremos enseguida que $\otimes$ es conmutativa, no hace falta verificar la distributividad lateral.

$$a \otimes (b \oplus c) \;=\; a \otimes (b+c+1) \;=\; a(b+c+1)+a+b+c+1 = ab+ac+2a+b+c+1 = (a \otimes b) \oplus (a \otimes c).$$

Ya tenemos pues que $(\mathbf{Z}, \oplus, \otimes)$ es un anillo. Veamos finalmente que es un dominio de integridad.
$\otimes$ Conmutativa: Elemental.
$\otimes$ admite neutro (unidad): Qué raro!! $\forall a \in \mathbf{Z}, \quad a \otimes 0 = 0 \otimes a = a \cdot 0 + a + 0 = a.$
$\otimes$ no tiene divisores de cero: Si $a, b \in \mathbf{Z}$ son tales que $a \otimes b = -1$, entonces
$-1 = ab + a + b = (a+1)(b+1) - 1$, lo que implica que $(a+1)(b+1) = 0$,
i.e., $a = -1$, ó, $b = -1$. ♣

Ex. 293 *Sea $(A, +, \cdot)$ un anillo. En A definimos: $a * b = ab + ba, \quad a, b \in A$.*
a) Estudiar las condiciones bajo las que $(A, +, *)$ es un anillo.
b) Si $(A, +, \cdot)$ es unitario, dar condiciones bajo las que $(A, +, *)$ es también unitario.

≡
a) Vamos a demostrar que

$$(A, +, *) \text{ es anillo} \;\Leftrightarrow\; \forall a, b, c \in A, \quad a(bc - cb) = (bc - cb)a.$$

[$\Rightarrow$] Suponiendo que $(A, +, *)$ es un anillo, sean a, b, c elementos arbitrarios de A. Como $*$ es asociativa

$$(b*a)*c = b*(a*c) \;\rightarrow\; (ab+ba)c + c(ab+ba) = b(ac+ca) + (ac+ca)b \;\rightarrow\; abc+cba = bca+acb.$$

Por tanto $a(bc - cb) = (bc - cb)a$.
[$\Leftarrow$] Razonando justo al revés de lo hecho arriba se demuestra que $*$ es asociativa. Como que es estable es inmediato, veamos que es distributiva (lo hacemos sólo por la izquierda):

$$\left.\begin{array}{l} a * (b+c) = a(b+c) + (b+c)a = ab + ac + ba + ca \\ a * b + a * c = ab + ba + ac + ca \end{array}\right\} \;\rightarrow\; a * (b+c) = a * b + a * c.$$

b) Veamos seguidamente que

$$(A, +, *) \text{ es unitario} \;\Leftrightarrow\; \exists x \in A \text{ tal que } x + x = 1.$$

[$\Rightarrow$] Suponiendo que $(A,+,*)$ es un anillo unitario, sea x su elemento unidad. Entonces

$$1 \;=\; x*1 \;=\; x\cdot 1+1\cdot x \;=\; x+x.$$

[$\Leftarrow$] Sea $x\in A$ tal que $x+x=1$. Veamos primero que no puede existir elemento alguno $a\in A$, $a\neq 0$, tal que $a+a=0$. De existir, tendríamos

$$1=x+x \;\rightarrow\; a=a(x+x)=ax+ax=(a+a)x=0\cdot x=0 \text{ Absurdo.}$$

Conviene observar que en todo anillo: $0\cdot x+0\cdot x=(0+0)x=0\cdot x\rightarrow\; 0\cdot x=0$. Ahora, para todo $a\in A$

$$x+x=1 \;\rightarrow\; \left\{\begin{array}{l} ax+ax=a \\ xa+xa=a \end{array}\right\} \;\rightarrow\; (ax-xa)+(ax-xa)=0 \overset{(visto\ arriba)}{\rightarrow} ax=xa.$$

Luego

$$\left\{\begin{array}{lllllllll} x*a &=& xa+ax &=& ax+ax &=& a(x+x) &=& a\cdot 1 &=& a \\ a*x &=& ax+xa &=& ax+ax &=& a(x+x) &=& a\cdot 1 &=& a \end{array}\right\} \;\rightarrow\; x*a=a*x=a.$$

Es decir, x es la unidad de $(A,+,*)$. ♣

Ex. 294 *Sea $(A,+,\cdot)$ un anillo. En el producto cartesiano $\mathbf{Z}\times A$ definimos*

$$(m,a)+(n,b) \;=\; (m+n,a+b);\quad (m,a)\cdot(n,b) \;=\; (mn,ab+na+mb).$$

Demostrar que $(\mathbf{Z}\times A,+,\cdot)$ es un anillo unitario.

$\equiv$
Para $(\mathbf{Z}\times A,+)$:
Estable: Evidente.
Asociativa: Evidente.
Neutro: Es $(0,0)$. Observar que el primer cero es un número entero, mientras que el segundo cero es el neutro de $(A,+)$.
Simétricos: $-(m,a)=(-m,-a)$.
Conmutativa: Evidente.
Para $(\mathbf{Z}\times A,\cdot)$:
Estable: Evidente.
Asociativa: Veámoslo

$$\left\{\begin{array}{l} [(m,a)(n,b)](p,c)=(mn,ab+na+mb)(p,c) \\ =(mnp,(ab+na+mb)c+p(ab+na+mb)+mnc) \\ \\ (m,a)[(n,b)(p,c)]=(m,a)(np,bc+pb+nc) \\ =(mnp,a(bc+pb+nc)+npa+m(bc+pb+nc)) \end{array}\right.$$

$$\left\{\begin{array}{l} =(mnp,abc+nac+mbc+pab+pna+pmb+mnc) \\ =(mnp,abc+pab+nac+npa+mbc+mpb+mnc). \end{array}\right.$$

Distributivas: Primero por la izquierda

$$\begin{cases} (m,a)[(n,b)+(p,c)] = (m,a)(n+p,b+c) = (m(n+p), a(b+c)+(n+p)a+m(b+c)) \\ (m,a)(n.b)+(m,a)(p.c) = (mn, ab+na+mb)+(mp, ac+pa+mc) \end{cases}$$

$$\begin{cases} = (mn+mp, ab+ac+na+pa+mb+mc) \\ = (mn+mp, ab+ac+na+pa+mb+mc). \end{cases}$$

Ahora por la derecha

$$\begin{cases} [(m,a)+(n,b)](p,c) = (m+n, a+b)(p,c) = ((m+n)p, (a+b)c+p(a+b)+(m+n)c) \\ (m,a)(p,c)+(n,b)(p.c) = (mp, ac+pa+mc)+(np, bc+pb+nc) \end{cases}$$

$$\begin{cases} = (mp+np, ac+bc+pa+pb+mc+nc) \\ = (mp+np, ac+bc+pa+pb+mc+nc). \end{cases}$$

Unitario: La unidad del anillo $(\mathbf{Z}\times A,+,\cdot)$ es $(1,0)\in\mathbf{Z}\times A$, ya que

$$\forall (m,a)\in \mathbf{Z}\times A,\quad (1,0)(m,a) \;=\; (m,0+a+0) \;=\; (m,a) \;=\; (m,a)(1,0).\ \clubsuit$$

Ex. 295 *Demostrar que, al desarrollar $(a+1)(b+1)$ según las dos formas conocidas, la propiedad conmutativa de la suma es deducible a partir de las demás condiciones de anillo.*

≡

Se trata de demostrar la propiedad conmutativa de la suma en $(A,+,\cdot)$ a partir de las propiedades distributivas y la unidad. Así, dados $a,b\in A$

$$\left.\begin{array}{l} (a+1)(b+1) = (a+1)b+a+1 = ab+b+a+1 \\ (a+1)(b+1) = a(b+1)+b+1 = ab+a+b+1 \end{array}\right\} \;\rightarrow\; b+a=a+b.\ \clubsuit$$

Ex. 296 *Demostrar que la propiedad conmutativa del producto en un anillo A equivale a que se cumpla*

$$\forall a,b\in A,\quad (a+b)^2 \;=\; a^2+2ab+b^2.$$

≡

[$\Rightarrow$] Si $(A,+,\cdot)$ es un anillo conmutativo, entonces, dados $a,b\in A$

$$(a+b)^2 \;=\; (a+b)(a+b) \;=\; a(a+b)+b(a+b) \;=\; a^2+ab+ba+b^2 \;=\; a^2+2ab+b^2.$$

[$\Leftarrow$] Si se cumple la igualdad anterior para dos elementos cualesquiera del anillo, entonces

$$\forall a,b\in A,\quad (a+b)^2 \;=\; a^2+2ab+b^2 \;\rightarrow\; a^2+ab+ba+b^2 \;=\; a^2+2ab+b^2 \;\rightarrow\; ab=ba.\ \clubsuit$$

Ex. 297 *Demostrar que en un anillo unitario el elemento unidad es único.*

≡

Sea $(A, +, \cdot)$ un anillo unitario con unidad $1 \in A$. Sea $x \in A$ tal que: $\forall a \in A, \quad xa = ax = a$. Entonces, tomando en particular $a := 1$, se tiene que $1 = a = ax = 1 \cdot x = x$. ♣

Ex. 298 *En un anillo unitario A, un elemento $u \in A$ se dice inversible siempre existe un elemento $u^{-1} \in A$ tal que $u \cdot u^{-1} = u^{-1} \cdot u = 1$. Demostrar ningún elemento inversible es divisor de cero.*

≡

Sea $u \in A$ un elemento inversible. Entonces Si $a \in A$ es tal que $ua = 0$, se tiene que $a = u^{-1}ua = 0$. Ello implica que u no es divisor de cero. ♣

Ex. 299 *Demostrar que el producto de un divisor de cero por un elemento cualquiera de un anillo es otro divisor de cero.*

≡

Sea $a \in A$ un divisor de cero. Sea $x \in A$. Al ser a un divisor de cero existe $b \in A, \ b \neq 0$, tal que $ab = 0$. Así $(xa)b = x(ab) = x \cdot 0 = 0$. Luego xa es un divisor de cero. ♣

Nota 33 En el ejercicio previo, al decir divisor de cero se entiende que es un elemento $a \in A$ (sea cero, o no) tal que existe un $b \in A, \ b \neq 0$, con $a \cdot b = 0$.

Ex. 300 *Sean a, b elementos de un anillo A tales que su producto ab es divisor de cero. Demostrar que alguno de ellos, a ó b, ha de ser divisor de cero.*

≡

Usamos la definición de divisor de cero dada arriba. Si ab es divisor de cero, existe $c \in A, \ c \neq 0$, tal que $(ab)c = 0$. Entonces

$$0 = (ab)c = a(bc) \rightarrow \begin{cases} \text{Si } bc \neq 0 \rightarrow a \text{ es div. de } 0 \\ \text{Si } bc = 0 \rightarrow b \text{ es div. de } 0. \end{cases} \clubsuit$$

Ex. 301 *Dar ejemplos que demuestren que la suma de divisores de cero no es necesariamente un divisor de cero.*

≡

Damos un par de ejemplos.

Ejemplo 1 En el anillo $\mathbf{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$:

$\overline{2}$ y $\overline{3}$ son divisores de cero, pues $\overline{2} \cdot \overline{3} = \overline{0}$. Sin embargo $\overline{2} + \overline{3} = \overline{5}$ no es divisor de cero, ya que: $\overline{5} \cdot \overline{5} = \overline{1}$, demuestra que $\overline{5}$ es inversible en $\mathbf{Z}_6$.

Ejemplo 2 Consideremos el anillo $C[0,1]$ de las funciones continuas en $[0,1]$. Las funciones

$$f(x) = \begin{cases} 0, & x \in [0, \frac{1}{2}], \\ x - \frac{1}{2}, & x \in]\frac{1}{2}, 1] \end{cases}$$
$$g(x) = \begin{cases} \frac{1}{2} - x, & x \in [0, \frac{1}{2}], \\ 0, & x \in]\frac{1}{2}, 1] \end{cases}$$

son divisores de cero, pues $f \neq 0$, $g \neq 0$ y $fg = 0$. Sin embargo, la función suma

$$(f+g)(x) = f(x) + g(x) \ = \ \begin{cases} \frac{1}{2} - x, & x \in [0, \frac{1}{2}], \\ x - \frac{1}{2}, & x \in]\frac{1}{2}, 1] \end{cases}$$

no es un divisor de cero, como seguidamente demostramos: Claramente (dibujarla) $f + g \in C[0,1]$. Si $h \in C[0,1]$ es tal que $(f+g)h = 0$, entonces

$$\forall x \in [0,1] \setminus \{\frac{1}{2}\}, \quad 0 = [f(x) + g(x)]h(x) \overset{(f(x)+g(x)\neq 0)}{\to} h(x) = 0.$$

Por continuidad, ello garantiza que $h = 0$, por lo que $f + g$ no es divisor de cero . ♣

Ex. 302 *Dados dos anillos A_1 y A_2, se llama anillo producto de A_1 por A_2 a la estructura $(A_1 \times A_2, +, \cdot)$ con*

$$(a_1, a_2) + (b_1, b_2) \ = \ (a_1 + b_1, a_2 + b_2); \quad (a_1, a_n) \cdot (b_1, b_2) \ = \ (a_1 b_1, a_2 b_2).$$

a) Demostrar que $(A_1 \times A_2, +, \cdot)$ es un anillo.
b) Si A_1 y A_2 son dominios de integridad, demostrar con un contraejemplo que $A_1 \times A_2$ no tiene porqué serlo.

≡
a) $(A_1 \times A_2, +)$ es el producto directo de dos grupos abelianos, luego es otro grupo abeliano. Además, es bastante mecánico verificar todas las restantes condiciones de anillo para $(A_1 \times A_2, +, \cdot)$.
b) El contraejemplo que aportamos es el siguiente: Sean $A_1 = A_2 = \mathbf{Z}$. Claramente, $\mathbf{Z}$ es dominio de integridad. Sin embargo, $(1,0)$ y $(0,1)$ son divisores de cero en $\mathbf{Z} \times \mathbf{Z}$, por lo que este anillo no es íntegro. ♣

Ex. 303 *Si m, n son primos entre sí, demostrar que $\mathbf{Z}_m \times \mathbf{Z}_n \ \cong \ \mathbf{Z}_{mn}$.*

≡
Se trata de demostrar que ambos anillos son isomorfos, es decir, hay que construir un homomorfismo de anillos entre ambos que sea inyectivo y sobre. Así, definimos, woops... primero, al ser primos entre sí, del lema de Bezout sabemos que existen $p, q \in \mathbf{Z}$ tales que $pm + qn = 1$,

$$\begin{array}{rccc} \varphi & : & \mathbf{Z}_m \times \mathbf{Z}_n & \longrightarrow & \mathbf{Z}_{mn} \\ & & (\overline{a}, \overline{b}) & \to & \overline{qna + pmb}. \end{array}$$

φ bien definida: Hay que ver que la definición de cada imagen no depende de los representantes elegidos en las clases correspondientes. Así, sean $\overline{a} = \overline{a'} \in \mathbf{Z}_m$, $\overline{b} = \overline{b'} \in \mathbf{Z}_n$. Hay que ver que $\overline{qna + pmb} = \overline{qna' + pmb'}$ en $\mathbf{Z}_{mn}$.

$$\left.\begin{array}{l} \overline{a} = \overline{a'} \ \rightarrow \ \exists r \in \mathbf{Z} \ / \ a - a' = rm \\ \overline{b} = \overline{b'} \ \rightarrow \ \exists s \in \mathbf{Z} \ / \ b - b' = sn \end{array}\right\} \Rightarrow (qna + pmb) - (qna' + pmb')$$

$$= qn(a - a') + pm(b - b') = qnrm + pmsn = mn(qr + ps) = \overline{0} \in \mathbf{Z}_{mn}.$$

φ homomorfismo de anillos: Dados $(\overline{a}, \overline{b}), (\overline{c}, \overline{d}) \in \mathbf{Z}_m \times \mathbf{Z}_n$

$$\varphi[(\overline{a}, \overline{b}) + (\overline{c}, \overline{d})] = \varphi(\overline{a} + \overline{c}, \overline{b} + \overline{d}) == \overline{qn(a + c) + pm(b + d)}$$

$$= \overline{qna + qnc + pmb + pmd} = \overline{qna + pmb} + \overline{qnc + pmd} = \varphi(\overline{a}, \overline{b}) + \varphi(\overline{c}, \overline{d}).$$

$$\varphi[(\overline{a}, \overline{b})(\overline{c}, \overline{d})] = \varphi(\overline{ac}, \overline{bd}) = \overline{qnac + pmbd} \overset{(mirar \ abajo \ en \ (*))}{=}$$

$$= \overline{qna + pmb} \cdot \overline{qnc + pmd} = \varphi(\overline{a}, \overline{b})\varphi(\overline{c}, \overline{d}).$$

$$(*) \quad : \quad (qna + pmb)(qnc + pmd) = q^2n^2ac + pqadmn + pqbcmn + p^2m^2bd$$

$$\rightarrow \ (qnac+pmbd)-(qna+pmb)(qnc+pmd) = qnac+pmbd-q^2n^2ac-p^2m^2bd-mnpq(ad+bc)$$

$$= qnac(1 - qn) + pmbd(1 - pm) - mnpq(ad + bc) = pqacmn + pqbdmn - mnpq(ad + bc)$$

$$= pqmn(ac + bd - ad - bc) \ \rightarrow \ \text{En} \ \mathbf{Z}_{mn} : \ \overline{qnac + pmbd} = \overline{(qna + pmb)(qnc + pmd)}.$$

φ inyectiva: Sea $(\overline{a}, \overline{b}) \in Ker(\varphi)$, entonces

$$\overline{0} = \varphi(\overline{a}, \overline{b}) = \overline{qna + pmb} \ \rightarrow \ mn \mid (qna + pmb) \ \rightarrow \ \frac{qa}{m} + \frac{pb}{n} = \frac{qna + pmb}{mn} \in \mathbf{Z}.$$

Pero, $mcd(m, n) = 1$ implica que

$$\left.\begin{array}{l} \frac{qa}{m} \in \mathbf{Z} \ \rightarrow \ m \mid qa \overset{(mcd(m,q)=1)}{\rightarrow} m \mid a \rightarrow \overline{a} = \overline{0} \in \mathbf{Z}_m \\ \frac{pb}{n} \in \mathbf{Z} \ \rightarrow \ n \mid pb \overset{(mcd(n,p)=1)}{\rightarrow} n \mid b \rightarrow \overline{b} = \overline{0} \in \mathbf{Z}_n \end{array}\right\} \Rightarrow (\overline{a}, \overline{b}) = (\overline{0}, \overline{0}).$$

Al tratarse de una aplicación inyectiva entre dos conjuntos finitos del mismo cardinal, pues

$$card(\mathbf{Z}_m \times \mathbf{Z}_n) = card(\mathbf{Z}_m) \cdot card(\mathbf{Z}_n) = mn = card(\mathbf{Z}_{mn}),$$

se tiene que φ también es sobre. ♣

Ex. 304 *Sea A un anillo unitario y conmutativo. Determinar el grupo de los elementos unitarios (inversibles) del anillo de polinomios $A[x]$.*

$\equiv$

Recordemos que, en un anillo unitario $(A,+,\cdot)$, un elemento u se dice unitario, o inversible, siempre que existe $u^{-1} \in A$ tal que $uu^{-1} = u^{-1}u = 1$. Si indicamos mediante U_A al conjunto de los elementos unitarios de A, notar que, como $1 \in U_A$, se tiene que $U_A \neq \emptyset$. Lo que nos pide el ejercicio es que pongamos condiciones para hallar $U_{A[x]}$. Demostramos seguidamente que

$$f(x) = a_0 + a_1x + ... + a_nx^n \in U_{A[x]} \Leftrightarrow \begin{cases} a_0 \in U_A \\ \exists k \in \mathbf{N} \ / \ (a_1x + a_2x^2 + ... + a_nx^n)^k = 0. \end{cases}$$

[$\Rightarrow$] Si $f(x) = a_0 + a_1x + ... + a_nx^n \in U_{A[x]}$, entonces existe un polinomio en $A[x]$ $h(x) = b_0 + b_1x + ... + b_rx^r$ tal que $f(x)h(x) = 1$.Al multiplicar dichos polinomios, se deduce que $a_0b_0 = 1$, lo que prueba que $a_0 \in U_A$. Vcamos la scgunda condición. Sacando facotor común la mayor potencia de x posible, podemos escribir

$$a_1x + a_2x^2 + ... + a_nx^n = -x^m \cdot g(x), \quad g(x) \in A[x], \quad x \not| \ g(x).$$

Razonando por reducción al absurdo, supongamos que, para todo $k \in \mathbf{N}$, $(a_1x + a_2x^2 + ... + a_nx^n)^k \neq 0$. Obviamente $g(x)^k \neq 0, \forall k \in \mathbf{N}$. Para cada k, consideramos el polinomio

$$p_k(x) := 1 + b_0x^m g(x) + b_0^2x^{2m}g(x)^2 + ... + b_0^kx^{km}g(x)^k \overset{(prog.geom.)}{=} \frac{b_0^{k+1}x^{(k+1)m}g(x)^{k+1} - 1}{b_0x^mg(x) - 1}.$$

Entonces

$$f(x)p_k(x) = (a_0 - x^mg(x))p_k(x) = a_0(1 - b_0x^mg(x))p_k(x) = a_0[1 - b_0^{k+1}x^{(k+1)m}g(x)^{k+1}].$$

Como $f(x)h(x) = 1$, substituyendo arriba

$$f(x)[a_0h(x) - p_k(x)] = b_0^kx^{(k+1)m}g(x)^{k+1}.$$

Puesto que la igualdad anterior vale para todo k, tomando en particular $k \in \mathbf{N}$ de modo que $grado(h(x)) < grado(p_k(x))$, lo que es posible gracias a que sabemos que $g(x)^k \neq 0$, podemos utilizar la igualdad anterior para este valor de k. Entonces

$$x^{(k+1)m} \mid a_0h(x) - p_k(x) = ... - a_0^kx^{km}g(x)^k \rightarrow x^{(k+1)m} \mid x^{km}g(x)^k$$

$$\rightarrow x \mid g(x)^k \rightarrow x \mid g(x). \ Absurdo$$

[$\Leftarrow$] Asumiendo que $a_0 \in U_A$ y que, para un $k \in \mathbf{N}$, $(a_1x + a_2x^2 + ... + a_nx^n)^k = 0$, utilizando la nomenclatura anterior

$$p_{k-1}(x)(1 - a_0^{-1}x^mg(x)) = 1 - a_0^{-k}x^{km}g(x)^k = 1 + a_0^{-k}(a_1x + a_2x^2 + ... + a_nx^n)^k = 1.$$

Pero

$$1 - a_0^{-1}x^mg(x) = a_0^{-1}f(x) \Rightarrow f(x) \cdot [a_0^{-1}p_{k-1}(x)] = 1. \ i.e., \ f(x) \in U_{A[x]}. \ \clubsuit$$

Nota 34 Si A fuese un dominio de integridad, sabemos que $A[x]$ también lo sería. Por tanto, usando el ejercicio previo

$$f(x) = a_0 + a_1x + ... + a_nx^n \ \in \ U_{A[x]} \ \Leftrightarrow \quad f(x) = a_0 \in U_A,$$

ya que la condición $(a_1x + ... + a_nx^n)^k = 0$ implica que $a_1x + ... + a_nx^n = 0$, de donde $f(x) = a_0 \in U_A$. Es decir, cuando A es dominio de integridad los únicos polinomios inversibles de $A[x]$ son los elementos inversibles de A.

Observar que si A es un anillo unitario no íntegro, por ejemplo $\mathbf{Z}_4$, entonces hay polinomios unitarios (inversibles) que no son constantes: Tomar $f(x) := \overline{1} + \overline{2}x \in \mathbf{Z}_4[x]$

$$f(x)^2 \ = \ (\overline{1} + \overline{2}x)^2 = \overline{1}^2 + 2 \cdot \overline{2}x + \overline{2}^2x^2 = \overline{1}.$$

Ex. 305 *Indicar las condiciones que ha de verificar un anillo A para que se cumpla*

$$\forall f(x), g(x) \in A[x] \setminus \{0\}, \quad grado[f(x)g(x)] \ = \ grado(f(x)) \ + \ grado(g(x)).$$

$\equiv$

Demostramos que la propiedad descrita en el enunciado es equivalente a que el anillo A sca íntegro.

[$\Rightarrow$] Si A no fuese íntegro, sean $a, b \in A$, $a \neq 0$, $b \neq 0$, $ab = 0$. Consideremos los polinomios de $A[x]$

$$\left.\begin{array}{l} f(x) := \ 1 + ax \\ g(x) := \ 1 + bx \end{array}\right\} \ \rightarrow \quad f(x)g(x) \ = \ (1 + ax)(1 + bx) = 1 + (a + b)x$$

$$\rightarrow \left\{\begin{array}{l} grado(f(x)) = 1 \\ grado(g(x)) = 1 \\ grado(f(x) + g(x)) \leq 1 \neq 2 = grado(f(x)) + grado(g(x)). \end{array}\right.$$

[$\Leftarrow$] Asumiendo que A es íntegro, sean $f(x), g(x) \in A[x]$ tales que $grado(f(x)) = m$ y $grado(g(x)) = n$, respectivamente. Así, podemos expresarlos como

$$\left.\begin{array}{l} f(x) = a_0 + a_1x + ... + a_mx^m, \ a_m \neq 0 \\ g(x) = b_0 + b_1x + ... + b_nx^n, \ b_n \neq 0 \end{array}\right\} \ f(x)g(x) \ = \ a_0b_0 + (a_0b_1 + a_1b_0)x + ... + a_mb_nx^{m+n}.$$

De donde, como $a_mb_n \neq 0$, se tiene que $grado(f(x)g(x)) = m + n$. ♣

Ex. 306 *Sea A un anillo unitario y conmutativo. Consideramos el anillo de las series de potencias $A_\infty[x] = \{\sum_{n=0}^{\infty} a_nx^n : \ a_n \in A, \ n \geq 0\}$ visto en un ejercicio anterior. Determinar el grupo de elementos unitarios de $A_\infty[x]$.*

$\equiv$

Antes no lo hemos dicho, pues vamos a hablar de ello ahora. En un anillo unitario A, al hacer referencia a su conjunto de unitarios U_A se le da el calificativo de grupo, lo que se intenta indicar es que U_A es un grupo multiplicativo. Veamos que es así: Si

$u, v \in U_A$, entonces existen $u^{-1}, v^{-1} \in A$ tales que $uu^{-1} = vv^{-1} = 1$; así $(uv^{-1})(vu^{-1}) = u(vv^{-1})u^{-1} = u \cdot 1 \cdot u^{-1} = uu^{-1} = 1$, i.e., $uv^{-1} \in U_A$. Volvamos a nuestro ejercicio. Vamos a demostrar que

$$f(x) = \sum_{n=0}^{\infty} a_n x^n \in U_{A_\infty[x]} \Leftrightarrow a_0 \in U_A.$$

[$\Rightarrow$] Si $f(x) = \sum_{n=0}^{\infty} a_n x^n \in U_{A_\infty[x]}$, existe $h(x) = \sum_{n=0}^{\infty} b_n x^n \in A_\infty[x]$ tal que $f(x)h(x) = 1$. Eso implica que $a_0 b_0 = 1$, por lo que $a_0 \in U_A$.
[$\Leftarrow$] Supongamos que $a_0 \in U_A$. Escribimos

$$f(x) = a_0 + x \sum_{n=1}^{\infty} a_n x^{n-1}.$$

Consideramos $g(x) := -a_0^{-1} \sum_{n=1}^{\infty} a_n x^{n-1} \in A_\infty[x]$. Entonces $f(x) = a_0(1 - xg(x))$. Así

$$f(x) \cdot [a_0^{-1} \sum_{n=0}^{\infty} x^n g(x)^n]$$

$$= a_0(1 - xg(x))a_0^{-1} \sum_{n=0}^{\infty} x^n g(x)^n = (1 - xg(x))[1 + xg(x) + x^2 g(x)^2 + ...] = 1.$$

Por tanto $f(x) \in U_{A_\infty[x]}$. ♣

4.2. Ideales de un anillo

Ex. 307 *Demostrar que, si I y J son ideales del anillo A, entonces $I \cap J$ es otro ideal de A.*

≡

En un anillo $(A, +, \cdot)$, un subconjuto $I \subset A$ es un ideal por la izquierda (derecha) siempre que se cumplan las siguientes dos condiciones:

1) $(I, +)$ es subgrupo de $(A, +)$.

2) Si $x \in I$, entonces: $\forall a \in A$, $ax \in I$ (resp. $xa \in I$).

Cuando un subconjuto es ideal tanto por la izquierda como por la derecha, se dice que es un ideal bilátero. Claramente, si el anillo es conmutativo, todo ideal es bilátero.

Pasando al ejercicio, es evidente que $(I \cap J, +)$ es subgrupo de $(A, +)$, ya que de la teoría de grupos sabemos que la intersección de cualquier familia de subgrupos lo sigue siendo. Veamos la segunda condición (lo hacemos por la izquierda): Si $x \in I \cap J$ y $a \in A$, entonces

$$\left.\begin{array}{l} I \text{ ideal } \rightarrow \quad ax \in I \\ J \text{ ideal } \rightarrow \quad ax \in J \end{array}\right\} \Rightarrow \quad ax \in I \cap J. \clubsuit$$

Ex. 308 *En un anillo unitario conmutativo, dados los ideales I, J, K, demostrar las siguientes igualdades:*

a) $(I + J) + K = I + (J + K)$.

b) $I + (\ 0\ ) = I = (\ 0\ ) + I$.
c) $I + (\ 1\ ) = (\ 1\ ) = (\ 1\ ) + I$.
d) $I + J = J + I$.

$\equiv$
a)
[$\subset$] Si $x \in (I + J) + K$, existen $a \in I + J$, $b \in K$ tales que $x = a + b$. Pero, como $a \in I + J$, existen $u \in I$, $v \in J$, de modo que $a = u + v$. Así

$$x = a + b = (u + v) + b = u + (v + b) \in I + (J + K).$$

[$\supset$] Análogo a lo hecho antes.
b)
[$\subset$] Si $x \in I + (\ 0\ )$, entonces, como $(\ 0\ ) = \{0\}$, $x \in I$.
[$\supset$] Idem.
c) Esta igualdad es evidente, ya que $(\ 1\ ) = A$.
d)
[$\subset$] Si $x \in I + J$, entonces existen $a \in I$, $b \in J$ tales que $x = a + b = b + a$, al ser A conmutativo, lo que implica que $x \in J + I$.
[$\supset$] Idem. ♣

Ex. 309 *Demostrar que si un ideal contiene algún elemento unitario entonces es todo el anillo.*

$\equiv$
Sea A un anillo unitario y sea I un ideal de A (por la izquierda, por ejemplo). Supongamos que $u \in U_A \cap I$. Entonces

$$\forall a \in A, \quad a = a \cdot 1 = au^{-1}u = (au^{-1})u \in I \quad \Rightarrow \quad A = I. \clubsuit$$

Ex. 310 *Demostrar que, si I, J y K son ideales del anillo unitario conmutativo A, entonces*
a) $I \cap (J + K) \supset (I \cap J) + (I \cap K)$.
b) $I + (J \cap K) \subset (I + J) \cap (I + K)$.

$\equiv$
a) Si $x \in (I \cap J) + (I \cap K)$, existen $a \in I \cap J$, $b \in I \cap K$ tales que $x = a + b$. Entonces $x = a + b \in I$ y $x = a + b \in J + K$. Consecuentemente, $x \in I \cap (J + K)$.
b) Si $x \in I + (J \cap K)$, existen $a \in I$, $b \in J \cap K$ tales que $x = a + b$. Entonces $x = a + b \in I + J$ y $x = a + b \in I + K$. Consecuentemente, $x \in I \cap (I + J) \cap (I + K)$. ♣

Ex. 311 *Dado un subconjunto S de un anillo A unitario y conmutativo, se define el ideal generado por S como el menor ideal (aquí son todos biláteros) que contiene a S, se representa como $(\ S\ )$.*
a) Demostrar que

$$(\ S\ ) = \{\ a_1s_1 + a_2s_2 + ... + a_ns_n \ : \ n \in \mathbf{N},\ a_1, a_2, ..., a_n \in A,\ s_1, s_2, ..., s_n \in S\ \}.$$

b) Demostrar que $u \in U_A \Leftrightarrow (\ u\ ) = A$.

$\equiv$
a) Llamando

$$I_S \;=\; \{\; a_1s_1 + a_2s_2 + ... + a_ns_n \;:\; n \in \mathbf{N},\; a_1, a_2, ..., a_n \in A,\; s_1, s_2, ..., s_n \in S\},$$

todo consiste en ver que I_S es un ideal, que contiene a S y que es el menor posible.
I_S es ideal: Es inmediato que $(I_S, +)$ es subgrupo de $(A, +)$. Ahora, si $a \in A$ y $x \in I_S$, tenemos que existen $a_1, ..., a_n \in A$, $s_1, ..., s_n \in S$ tales que $x = a_1s_1 + ... + a_ns_n$. Así

$$ax \;=\; a(a_1s_1 + ... + a_ns_n) \;=\; (aa_1)s_1 + ... + (aa_n)s_n \;\in\; I_S.$$

I_S contiene a S: Si $s \in S$, $s = 1 \cdot s \in I_S$.
I_S es el menor ideal que contiene a S: Sea J un ideal de A conteniendo a S. Entonces

$$\forall x \in I_S,\; \exists a_1, ..., a_n \in A,\; \exists s_1, ..., s_n \in S \;/\; x = a_1s_1 + ...a_ns_n.$$

Como J es un ideal y $s_1, ..., s_n \in J$, se tiene que $x = a_1s_1 + ... + a_ns_n \in J$, es decir, $I_S \subset J$. b)
$[\Rightarrow]$ Si u es un elemento unitario, entonces

$$\forall a \in A, \quad a \;=\; a \cdot 1 \;=\; (au^{-1})u \;\in\; (\; u\;) \;\Rightarrow\; A = (\; u\;).$$

$[\Leftarrow]$ Si $(\; u\;) = A$, como $1 \in (\; u\;)$, existe $a \in A$ tal que $1 = au$, es decir, $u \in U_A$. ♣

Ex. 312 *Si* $(\; a_1, a_2, ..., a_n\;)$ *representa al menor ideal que contiene los elementos* $a_1, a_2, ..., a_n$, *demostrar que*

$$(\; a_1, a_2, ..., a_n\;) \;=\; (\; a_1\;) \;+\; (\; a_2\;) \;+\; ... \;+\; (\; a_n\;).$$

$\equiv$
$[\subset]$ Obvio, pues $a_1, a_2, ..., a_n \in (\; a_1\;) + (\; a_2\;) + ... + (\; a_n\;)$..
$[\supset]$ Sabemos que $(\; a_1\;) + (\; a_2\;) + ... + (\; a_n\;)$ es un ideal y que claramente contiene $a_1, a_2, ..., a_n$. Veamos que es el menor que lo cumple. Sea I un ideal de A tal que $a_i \in I$, $1 \leq i \leq n$.

$$\forall x \in \sum_{i=1}^{n}(\; a_i\;) \;\rightarrow\; \forall i = 1, 2, ..., n,\; \exists x_i \in (\; a_i) \;/\; x = \sum_{i=1}^{n} x_i$$

$$\rightarrow\; \forall i = 1, 2, ..., n,\; \exists b_i \in A \;/\; x_i = b_ia_i$$

Por tanto, como I es un ideal, $x = \sum_{i=1}^{n} b_ia_i \in I$. Hemos demostrado que $\sum_{i=1}^{n}(\; a_i\;) \subset I$, como se requería. ♣

Ex. 313 *Sea* A *un anillo unitario y conmutativo. Sean* $a, b \in A$.
a) Demostrar que: $(\; a\;) \subset (\; b\;) \;\Leftrightarrow\; \exists c \in A \;/\; a = bc.$
b) Demostrar que: $(\; a\;) = (\; b\;) \;\Leftrightarrow\; \exists u \in U_A \;/\; a = bu.$

$\equiv$

a)

$[\Rightarrow]$ Si $(\ a\ ) \subset (\ b\ )$, entonces, como $a \in (\ b\ )$, existe $c \in A$ tal que $a = bc$.

$[\Leftarrow]$ Si $a = bc$, con $c \in A$, dado $x \in (\ a\ )$, por lo visto antes, existe $d \in A$ de modo que $x = da$. Así $x = d(bc) = (cd)b$, lo que nos dice que $x \in (\ b\ )$.

b)

$[\Rightarrow]$ Si $(\ a\ ) = (\ b\ )$, entonces

$$\left.\begin{array}{l} (\ a\ ) \subset (\ b\ ) \overset{(aptdo.a))}{\rightarrow} \exists c \in A \ / \ a = bc \\ (\ b\ ) \subset (\ a\ ) \overset{(aptdo.a))}{\rightarrow} \exists d \in A \ / \ b = ad \end{array}\right\} \Rightarrow ab = (ab)(cd) \rightarrow cd = 1 \rightarrow \text{si } u := c \rightarrow a = ub.$$

$[\Leftarrow]$ Si $a = ub$, con $u \in U_A$, entonces

$$\left.\begin{array}{l} a = ub \ \rightarrow \ (\ a\ ) \subset (\ b\ ) \\ b = u^{-1}a \ \rightarrow \ (\ b\ ) \subset (\ a\ ) \end{array}\right\} \Rightarrow \ (\ a\ ) = (\ b\ ). \clubsuit$$

Ex. 314 *En el anillo* $\mathbf{Z}$ *de los números enteros, demostrar que, si* $m, n \in \mathbf{N}$*, entonces*

a)

$$(\ m\ ) \cap (\ n\ ) = (\ mcm(m,n)\ ).$$

b)

$$(\ m\ ) + (\ n\ ) = (\ mcd(m,n)\ ).$$

$\equiv$

a)

$[\subset]$ Si $x \in (\ m\ ) \cap (\ n\ )$, entonces existen $a, b \in \mathbf{Z}$ de modo que $x = am = bn$. Ello implica que

$$\left.\begin{array}{l} m \mid x \\ n \mid x \end{array}\right\} \rightarrow \ mcm(m,n) \mid x \ \rightarrow \ x \in (\ mcm(m,n)\ ).$$

$[\supset]$ Si $x \in (\ mcm(m,n)\ )$, entonces existe $a \in \mathbf{Z}$ tal que $x = a \cdot mcm(m,n)$. Llamando, por comodidad, $M := mcm(m,n)$, tenemos que

$$M \mid x \ \rightarrow \ m \mid x \ \wedge \ n \mid x \ \Rightarrow \ x \in (\ m\ ) \cap (\ n\ ).$$

b) Llamemos por comodidad $d := mcd(m,n)$. Entonces

$[\subset]$

$$\left.\begin{array}{l} d \| \ m \ \rightarrow \ m \in (\ d\ ) \\ d \| \ n \ \rightarrow \ n \in (\ d\ ) \end{array}\right\} \Rightarrow \left\{\begin{array}{l} (\ m\ ) \subset (\ d\ ) \\ (\ n\ ) \subset (\ d\ ) \end{array}\right\} \Rightarrow \ (\ m\ ) + (\ n\ ) \subset (\ d\ ).$$

$[\supset]$ Al ser $d = mcd(m,n)$, existen $a, b \in \mathbf{Z}$ de modo que $d = am + bn$. Claramente $d = am + bn \in (\ m\ ) + (\ n\ )$. $\clubsuit$

Ex. 315 *Si I, J, K son ideales en un anillo A unitario y conmutativo, demostrar las siguientes propiedades del producto de idales*

a) $(IJ)K = I(JK)$.
b) $I(\ 1\ ) = I = I(\ 1\ )$.
c) $IJ = JI$.
d) $IJ \subset I \cap J)$.
e) $(\ a\ )(\ b\ ) = (\ ab\ )$.
f) $I(J + K) = IJ + IK$.
g) Si I, J cumplen que $I + J = A$, entonces $IJ = I \cap J$.

$\equiv$

Recordemos antes la definición de un producto de ideales

$$IJ \ = \ \{ \sum_{i=1}^{n} x_i y_i \ : \ n \in \mathbf{N},\ x_i \in I,\ y_i \in J,\ 1 \leq i \leq n \ \}.$$

De hecho se trata del menor ideal que contiene el conjunto $\{\ ab\ :\ a \in I,\ b \in J\ \}$.
a)
$[\ \subset\ ]$ Dado $x \in (IJ)K$, existen $n \in \mathbf{N}$, $y_i \in IJ$, $z_i \in K$, $1 \leq i \leq n$, tales que $x = \sum_{i=1}^{n} y_i z_i$. Para cada $i = 1, 2, ..., n$, como $y_i \in IJ$, existen $m_i \in N$, $u_{ij} \in I$, $v_{ij} \in J$ tales que $y_i = \sum_{j=1}^{m_i} u_{ij} v_{ij}$. Así

$$x \ = \ \sum_{i=1}^{n} y_i z_i \ = \ \sum_{i=1}^{n} (\sum_{j=1}^{m_i} u_{ij} v_{ij}) z_i \ = \ \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m_i}} u_{ij} v_{ij} z_i.$$

De la propiedad asociativa se desprende que la última suma están en $I(JK)$.
$[\ \subset\ ]$ Análogo a lo anterior.
b) $I(\ 1\ ) = IA = I = AI = (\ 1\ )I$.
c) Evidente, al tratarse de un anillo conmuativo.
d) Si $x \in IJ$, existen $n \in \mathbf{N}$, $y_i \in I$, $z_i \in$, $1 \leq i \leq n$, tales que $x = \sum_{i=1}^{n} y_i z_i$. Entonces, para cada $i = 1, 2, ..., n$, por definición de ideal,

$$\left.\begin{array}{l} y_i z_i \ \in \ I \\ y_i z_i \ \in \ J \end{array}\right\} \rightarrow \ \ y_i z_i \ \in \ I \cap J.$$

Luego $x = \sum_{i=1}^{n} y_i z_i \in \ I \cap J$.
e)
$[\ \subset\ ]$ Si $x \in (\ a\ )(\ b\ )$, entonces existen $n \in \mathbf{N}$, $y_i, z_i \in A$, $1 \leq i \leq n$, tales que $x = \sum_{i=1}^{n} (y_i a)(z_i b)$. Pero, claramente

$$x \ = \ \sum_{i=1}^{n} (y_i a)(z_i b) = \ (\sum_{i=1}^{n} y_i z_i) ab \ \in \ \ (\ ab\ ).$$

$[\ \supset\ ]$ Obvio.

f)
[$\subset$] Si $x \in I(J+K)$, entonces existen $n \in \mathbf{N}$, $y_i \in I$, $z_i \in J+K$, $1 \leq i \leq n$, de modo que $x = \sum_{i=1}^{n} y_i z_i$. Para cada $i = 1, 2, ..., n$, como $z_i \in J+K$, existen $u_i \in J$, $v_i \in K$ tales que $z_i = u_i + v_i$. Así

$$x = \sum_{i=1}^{n} y_i z_i = \sum_{i=1}^{n} y_i(u_i + v_i) = \sum_{i=1}^{n} y_i u_i + \sum_{i=1}^{n} y_i v_i \in (IJ) + (IK).$$

[$\supset$] Análogo.
g) Vimos anteriormente que $IJ \subset I \cap J$,por tanto, sólo hay que demostrar la inclusión recíproca. Sea $x \in I \cap J$. Como $I + J = A$, existen $a \in I$, $b \in J$ tales que $1 = a + b$. Entonces

$$x = x(a+b) = xa + xb \in IJ. \clubsuit$$

Ex. 316 *Si i, J son ideales del anillo A unitario y conmutativo, se define el ideal cociente como*

$$I : J = \{ x \in A : xb \in I, \forall b \in J \}.$$

Demostrar que $I : J$ es ideal de A.

$\equiv$
Si $x, y \in I : J$, queremos ver que $x - y \in I : J$. Aplicando la definición

$$\forall b \in J, \left\{ \begin{array}{l} bx \in I \\ by \in I \end{array} \right\} \rightarrow b(x-y) = bx - by \in I.$$

Finalmente, si $a \in A$, $x \in I : J$, dado $b \in J$, tenemos que $b(ax) = (ba)x \in I$, ya que I, J son ideales. Por tanto, $ax \in I : J$. $\clubsuit$

Ex. 317 *Demostrar las siguientes propiedades del cociente de ideales*
a) $(I : J)J \subset I$.
b) $(I : J) : K = I : (JK)$.
c) $I : (J+K) = (I : J) \cap (I : K)$.
d) $(I \cap J) : K = (I : K) \cap (J : K)$.
e) $I : J = A$ *si y sólo si* $I \supset J$.

$\equiv$
a) Dado $x \in I : J$, $\forall b \in J$, $xb \in I \rightarrow (I : J)J \subset I$.
b)
[$\subset$] Si $x \in (I : J) : K$, entonces $\forall y \in JK$, existen $n \in \mathbf{N}$, $a_1, ..., a_n \in J$, $b_1, ..., b_n \in K$ tales que $y = \sum_{i=1}^{n} a_i b_i$. Así

$$xy = x \sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} a_i (x b_i) \overset{(xb_i \in I:J)}{\in} I.$$

Por tanto $x \in I : (JK)$.

[$\supset$] Si $x \in I : (JK)$, $\forall y \in K$, veamos que $xy \in I : J$. Para ello, sea $z \in J$, entonces

$$(xy)z \;=\; x(yz) \overset{(yz \in JK)}{\in} I.$$

c)
[$\subset$] Si $x \in I : (J + K)$, $\forall y \in J$, como $J \subset J + K$, se tiene que $xy \in I$, luego $x \in I : J$. Análogamente se vé que $x \in I : K$.
[$\supset$] Si $x \in (I : J) \cap (I : K)$, $\forall y \in J$, $\forall z \in K$,

$$x(y + z) \;=\; xy + xz \;\in\; I + I \;=\; I.$$

Luego $x \in I : (J + K)$.
d)
[$\subset$] Si $x \in (I \cap J) : K$, $\forall y \in K$, tenemos que $xy \in I \cap J$. Luego $x \in (I : K) \cap (J : K)$.
[$\supset$] Si $x \in (I : K) \cap (J : K)$, $\forall y \in K$,

$$\left.\begin{array}{l} xy \in I \\ xy \in J \end{array}\right\} \;\rightarrow\; xy \in I \cap J.$$

Luego $x \in (I \cap J) : K$.
e)
[$\Rightarrow$] Suponiendo que $I : J \;=\; A$, sea $x \in J$. Entonces, como $1 \in I : J$

$$x \;= 1 \cdot x \in \; I \;\Rightarrow\; J \;\subset I.$$

[$\Leftarrow$] Si $J \subset I$, entonces, dado $x \in A$, $\forall y \in J$, está claro que $xy \;\in\; J \subset I$, luego $xy \in I$, de donde $x \in I : J$. ♣

Ex. 318 *Sea D un dominio de integridad. Sean $a, b \in D$. Demostrar que $I \;=\; \{\; x \in D \;:\; ax \in (\; b \;)\;\}$ es un ideal de D.*

≡
Sean $x, y \in I$, entonces

$$\left.\begin{array}{l} ax \in \;(\; b \;) \;\rightarrow\; \exists r \in D \;/\; ax = rb \\ ay \in \;(\; b \;) \;\rightarrow\; \exists s \in D \;/\; ay = sb \end{array}\right\} \;\rightarrow\; a(x - y) \;=\; (r - s)b \;\rightarrow\; x - y \in I.$$

Ello garantiza que $(I, +)$ es un subgrupo de $(D, +)$. Finalmente, si $x \in I$, $\forall d \in D$

$$ax \in \;(\; b \;) \;\rightarrow\; \exists r \in D \;/\; ax = rb \;\rightarrow\; a(dx) = drb \in (\; b \;) \;\rightarrow\; dx \in I.$$

Luego I es ideal de D. ♣

Ex. 319
a) Demostrar que todo ideal de $\mathbf{Z}_n$ es primcipal.
b) Determinar cuando es $\mathbf{Z}_n$ un dominio de ideales primcipales.

$\equiv$

a) Recordemos que en un anillo unitario y conmutativo A, un ideal I es principal siempre que existe $a \in A$ tal que $I = (\ a\ )$. Así, sea I un ideal de $\mathbf{Z}_n$. Suponemos que $I \neq \{0\}$, de lo contrario $I = (\ 0\ )$. Sea

$$k := \text{mín}\{\ x \in \mathbf{N} \ :\ x \neq 0,\ \overline{x} \in I\ \}.$$

Veamos que $I = (\ \overline{k}\ )$:

$[\ \supset\ ]$ Evidente, pues, por definición de k, se tiene que $\overline{k} \in I$.

$[\ \subset\ ]$ Dado $\overline{x} \in I$, podemos tomar sin perder generalidad $x > 0$ (si $\overline{x} = \overline{0}$, es inmediato que pertenece a $(\ \overline{k}\ )$). Entonces $k \leq x$, por lo que aplicando el algoritmo de la división entera: $\exists c, r \in \mathbf{N}$ tales que $x = ck + r$, $0 \leq r < k$. Así

$$\overline{x} = \overline{c} \cdot \overline{k} + \overline{r} \ \rightarrow\ \overline{r} = \overline{x} - \overline{c} \cdot \overline{k} \in I.$$

Pero, de nuevo de la definición de k, ello obliga a que $r = 0$. Por tanto, $\overline{x} = \overline{c}\overline{k}$, es decir, $\overline{x} \in (\ \overline{k}\ )$.

b) Por definición, un anillo es un dominio de ideales principales siempre que se trate de un dominio de integridad en donde todo ideal es principal. Así, como es bien sabido que $\mathbf{Z}_n$ es dominio de integridad si y sólo si n es un número primo, del apartado a) de este ejercicio concluimos que

$$\mathbf{Z}_n \text{ es dominio de ieales principales } \Leftrightarrow \ n \text{ es primo. } \clubsuit$$

Ex. 320 *Demostrar que, si A_1, A_2 son anillos unitarios conmutativos, entonces todo ideal del anillo producto $A_1 \times A_2$ es de la forma $I_1 \times I_2$, siendo I_1 e I_2 ideales de A_1 y de A_2, respectivamente.*

$\equiv$

Sea I un ideal del anillo producto $A_1 \times A_2$. Consideremos los conjuntos

$$\begin{aligned} I_1 &:= \{\ x_1 \in A_1 \ :\ (x_1, 0) \in I\ \} \\ I_2 &:= \{\ x_2 \in A_2 \ :\ (0, x_2) \in I\ \}. \end{aligned}$$

Veamos que I_1 e I_2 son ideales de A_1 y de A_2, respectivamente.

$$x_1, y_1 \in I_1,\ a_1 \in A_1 \rightarrow \left\{ \begin{array}{l} (x_1 - y_1, 0) = (x_1, 0) - (y_1, 0) \in I \ \rightarrow\ x_1 - y_1 \in I_1 \\ (a_1 x_1, 0) = (a_1, 0)(x_1, 0) \in I \ \rightarrow\ a_1 x_1 \in I_1 \end{array} \right.$$

$$x_2, y_2 \in I_2,\ a_2 \in A_2 \rightarrow \left\{ \begin{array}{l} (0, x_2 - y_2) = (0, x_2) - (0, y_2) \in I \ \rightarrow\ x_2 - y_2 \in I_2 \\ (0, a_2 x_2) = (0, a_2)(0, x_2) \in I \ \rightarrow\ a_2 x_2 \in I_2. \end{array} \right.$$

Finalmente probamos que $I = I_1 \times I_2$.

$[\subset\ ]$ Si $(x_1, x_2) \in I$, entonces

$$\left. \begin{array}{l} (x_1, 0) = (1, 0)(x_1, x_2) \in I \ \rightarrow\ x_1 \in I_1 \\ (0, x_2) = (0, 1)(x_1, x_2) \in I \ \rightarrow\ x_2 \in I_2 \end{array} \right\} \ \Rightarrow\ (x_1, x_2) \in I_1 \times I_2.$$

$[\supset\ ]$ Si $(x_1, x_2) \in I_1 \times I_2$, entonces

$$\left. \begin{array}{l} x_1 \in I_1 \ \rightarrow\ (x_1, 0) \in I \\ x_2 \in I_2 \ \rightarrow\ (0, x_2) \in I \end{array} \right\} \ \Rightarrow\ (x_1, x_2) = (x_1, 0) + (0, x_2) \in I. \ \clubsuit$$

Ex. 321 *Sea D un dominio de integridad. Demostrar que, para $n \geq 2$, $D[x_1, x_2, ..., x_n]$ no es dominio de ideales principales.*

$\equiv$

Recordemos que $D[x_1, x_2, ..., x_n]$ es el dominio de integridad (al serlo D) de los polinomios de coeficientes en D con indeterminadas $x_1, x_2, ..., x_n$. Por tanto, para ver que no es un dominio de ideales principales habrá que encontrar un ideal que no sea principal. Sea

$$I := \{ f(x_1, ..., x_n) \in D[x_1, ..., x_n] : f(0, 0, ..., 0) = 0 \}.$$

Veamos que I es un ideal de $D[x_1, ..., x_n]$: Si $f(x_1, ..., x_n), g(x_1, ..., x_n) \in I$, $h(x_1, ..., x_n) \in D[x_1, ..., x_n]$, entonces

$$\begin{cases} f(0, ..., 0) - g(0, ..., 0) = 0 - 0 = 0 \rightarrow f(x_1, ..., x_n) - g(x_1, ..., x_n) \in I \\ h(0, ..., 0) \cdot f(0, ..., 0) = 0 \rightarrow h(x_1, ..., x_n) f(x_1, ..., x_n) \in I. \end{cases}$$

Para ver que I no es un ideal principal razonamos por reducción al absurdo. Supongamos que I es principal, entonces existe $h(x_1, ..., x_n) \in D[x_1, ..., x_n]$ tal que $I = (h(x_1, ..., x_n))$. Ahora consideremos los siguientes dos elementos distintos de I (distintos, ya que $n \geq 2$)

$$f(x_1, ..., x_n) := x_1; \quad g(x_1, ..., x_n) := x_n \Rightarrow f(x_1, ..., x_n), g(x_1, ..., x_n) \in I.$$

Así

$$\begin{aligned} & f(x_1, .., x_n) \in I = (h(x_1, .., x_n)) \\ & \rightarrow \exists p(x_1, ..., x_n) \in D[x_1, .., x_n] / h(x_1, .., x_n) \cdot p(x_1, .., x_n) = x_1 \end{aligned}$$

$$\begin{aligned} & g(x_1, .., x_n) \in I = (h(x_1, ..., x_n)) \\ & \rightarrow \exists q(x_1, ..., x_n) \in D[x_1, .., x_n] / h(x_1, .., x_n) \cdot q(x_1, .., x_n) = x_n. \end{aligned}$$

Ello implica, ya que $h(x_1, ..., x_n)$ no puede ser constante, que existen a, b elementos unitarios de D tales que

$$\left.\begin{array}{l} p(x_1, ..., x_n) = a \rightarrow f(x_1, ..., x_n) = a h(x_1, ..., x_n) \rightarrow h(x_1, ..., x_n) = a^{-1} x_1 \\ q(x_1, ..., x_n) = b \rightarrow g(x_1, ..., x_n) = b h(x_1, ..., x_n) \rightarrow h(x_1, ..., x_n) = b^{-1} x_n \end{array}\right\}.$$

Así tenemos que $a^{-1} x_1 = b^{-1} x_n$, Absurdo. ♣

Ex. 322 *En* $\mathbf{Z}$, *calcular los ideales siguientes*

a) $(2) + (3)$.
b) $(2) + (4)$.
c) $(2) \cap [(3) + (4)]$.
d) $(2)[(3) \cap (4)]$.
e) $(2)(3) \cap (3)(4)$.
f) $(6) \cap (8)$.
g) $(6)(8)$.
h) $(6) : (2)$.
i) $(2) : (6)$.
j) $(2) : (3)$.

$\equiv$
a) $(2)+(3) = (1) = \mathbf{Z}$.
b) $(2)+(4) = (2)$.
c) $(2)\cap[(3)+(4)] = (2)\cap\mathbf{Z} = (2)$.
d) $(2)[(3)\cap(4)] = (2)(12) = (24)$.
e) $(2)(3) \cap (3)(4) = (6)\cap(8) = (24)$.
f) $(6)\cap(8) = (24)$.
g) $(6)(8) = (48)$.
h)

$$(6):(2) = \{x\in\mathbf{Z}:\ \forall y\in\mathbf{Z},\ 2yx\in(6)\} = \{x\in\mathbf{Z}:\ \forall y\in\mathbf{Z},\ yx\in(3)\} = (3).$$

i)

$$(2):(6) = \{x\in\mathbf{Z}:\ \forall y\in\mathbf{Z},\ 6yx\in(2)\} = \mathbf{Z}.$$

j)

$$(2):(3) = \{x\in\mathbf{Z}:\ \forall y\in\mathbf{Z},\ 3yx\in(2)\} = \{x\in\mathbf{Z}:\ \forall y\in\mathbf{Z},\ 2\mid xy\} = (2).\ \clubsuit$$

Ex. 323 *Sea* $\mathbf{Q}[x,y]$ *el anillo de los polinomios en las variables* x, y *sobre* $\mathbf{Q}$. *Calcular los siguientes ideales expresándolos en la forma* $(f_1(x,y), f_2(x,y), ..., f_n(x,y))$.

a) $(x)\cap(y)$.
b) $(x+y)^2$.
c) $(x,y)^2$.
d) $(x^2)\cap(x,y)$.
e) $(x^2+xy)\cap(xy+y^2)$.
f) $(x)+(y)$.
g) $(x+1)+(x)$.
h) $(x^2+xy)(x-y)$.
i) $(x^2)\cap[(xy)+(y^2)$.
j) $(x-y)\cap[(x)+(y^2)$.
k) $(xy):(y)$.
l) $(x^n):(x^m)$.
m) $(x):(y)$.
n) $((x+y)^2):(x)$.
o) $(xy):(x,y)$.

$\equiv$
a) $(x)\cap(y) = (xy)$, pues

$$f(x,y)\in(x)\cap(y) \leftrightarrow \left\{\begin{array}{l} x\mid f(x,y)\\ y\mid f(x,y)\end{array}\right\} \leftrightarrow xy\mid f(x,y).$$

b) $((x+y)^2) = (x+y)(x+y) = ((x+y)^2)$, de un problema resuelto anteriormente.
c)

$$(x,y)^2 = (x,y)(x,y) = [(x)+(y)][(x)+(y)]$$

$= (x)^2 + (x)(y) + (y)(x) + (y)^2 = (x^2) + (xy) + (y^2) = (x^2, xy, y^2)$.

d) $(x^2) \cap (x, y) = (x^2)$.
e) $(x^2 + xy) \cap (xy + y^2) = (xy(x+y))$.
f) $(x) + (y) = (x, y)$.
g) $(x+1) + (x) = \mathbf{Q}[x, y]$, pues $\forall f(x, y \in \mathbf{Q}[x, y],\ f(x, y) = (x+1)f(x, y) - xf(x, y)$.
h) $(x^2 + xy)(x - y) = (x(x-y)(x+y))$.
i) $(x^2) \cap [(xy) + (y^2)] = (x^2) \cap (xy, y^2) = (x^2 y)$.
j) $(x - y)[(x) + (y^2)] = (x(x-y)) + (y^2(x-y)) = (x(x-y), y^2(x-y))$.
k) $(xy) : (y) = \{ f(x, y) \in \mathbf{Q}[x, y] :\ \forall g(x, y) \in \mathbf{Q}[x, y],\ yf(x, y)g(x, y) \in (xy) \} = (x)$.
l) $(x^n) : (x^m) = \begin{cases} (x^{n-m}), & si\ n > m, \\ \mathbf{Q}[x, y], & si\ n \leq m. \end{cases}$
m) $(x) : (y) = (x)$.
n) $(x + y)^2 : (x) = ((x+y)^2) : (x) = \{f(x, y) \in \mathbf{Q}[x, y] :\ \forall g(x, y) \in \mathbf{Q}[x, y],\ (x+y)^2 \mid xf(x, y)g(x, y)\} = ((x+y)^2)$.
o) $(xy) : (x, y) = (xy)$. ♣

Ex. 324 *Demostrar que en* $\mathbf{Z}$ *el ideal* (n) *es primo si y sólo si* $n \in \{0, \pm 1\}$, *ó,* $|n|$ *es primo.*

≡

Recordemos que en un anillo unitario y conmutativo A un ideal I es un ideal primo siempre que

$$xy \in I \ \Rightarrow \ \begin{cases} x \in I \\ \quad ó \\ y \in I. \end{cases}$$

[$\Rightarrow$] Supongamos que $n \notin \{0, \pm 1\}$ y que $|n|$ no es primo. Entonces $|n| = pq$, $p, q \in \mathbf{N}$, $1 < p, q < |n|$. Claramente,

$$\left.\begin{array}{l} n \not| p \ \rightarrow \ p \notin (n) \\ n \not| q \ \rightarrow \ q \notin (n) \end{array}\right\} \ \Rightarrow \ (n) \text{ no es ideal primo.}$$

[$\Leftarrow$] Si $n = 0$, entonces $(0) = \{0\}$, que evidentemente es un ideal primo. Si $n = \pm 1$, entonces $(0) = A$, que también es ideal primo. Finalmente, supongamos que $|n|$ es primo. Sean $p, q \in \mathbf{Z}$ tales que $pq \in (n)$. Entonces

$$|n| \ | pq \ \rightarrow \ n \mid pq \overset{(|n| \text{ primo})}{\rightarrow} \left\{\begin{array}{ccc} n \mid p & \rightarrow & p \in (n) \\ ó & & ó \\ n \mid q & \rightarrow & p \in (n). \end{array}\right\} \ \Rightarrow \ (n) \text{ es ideal primo. } ♣$$

Ex. 325 *Demostrar que en* $\mathbf{Z}$ *todo ideal primo propio (es decir, distinto de* $\{0\}$ *y de* A*) es maximal.*

$\equiv$

En un anillo unitario y conmutativo A un ideal propio I es un ideal maximal siempre que, dado un ideal propio J, si $J \supset I$, entonces $J = I$. Es decir, un ideal es maximal cuando lo es dentro de la familia de ideales ordenada por inclusión. En $\mathbf{Z}$, supongamos que I es un ideal primo propio. Como $\mathbf{Z}$ es un dominio de ideales principales, existe $n \in \mathbf{N}$ tal que $I = (\ n\ )$. Del ejercicio anterior, sabemos que n es primo. Sea ahora J un ideal propio de $\mathbf{Z}$ tal que $J \supset I$. Dado $x \in J$, si $x \notin I = (\ x\ )$, ntonces $n \not| x$, de donde, por ser n primo, existen $p, q \in \mathbf{N}$ tales que $1 = pn + qx$. Así tenemos

$$\left.\begin{array}{l} 1 = pn + qx \\ pn \in (\ n\ ) = I \subset J \\ qx \in J \end{array}\right\} \Rightarrow\ 1 \in J\ \Rightarrow\ \ J = A\ \text{ Absurdo. } \clubsuit$$

Ex. 326 *Sea F un cuerpo y consideremos un polinomio $f(x) \in F[x]$.*

a) Demostrar que $(\ f(x)\ )$ es un ideal primo si y sólo si $f(x)$ es irreducible sobre F.

b) Averiguar cuándo es $(\ f(x)\ )$ un ideal maximal.

$\equiv$

a)

$[\ \Rightarrow\ ]$ Supongamos que $(\ f(x)\ )$ es un ideal primo. Supongamos también que $f(x)$ no es constante. Sean $g(x), h(x) \in F[x]$, $grado(g(x)) \geq 1$, $grado(h(x)) \geq 1$, tales que $f(x) = g(x)h(x)$. Entonces

$$\left.\begin{array}{l} 1 \leq grado(g(x)),\ grado(h(x)) < grado(f(x)) \\ g(x)h(x) \in (\ f(x)\ ) \\ g(x) \notin (\ f(x)\ ),\ g(x) \notin (\ f(x)\ ) \end{array}\right\} \Rightarrow\ (\ f(x\ ) \text{ no es ideal primo, Absurdo.}$$

$[\ \Leftarrow\ ]$ Si $f(x)$ es constante, evidentemente, suponiendo que $f(x) = c \in F$,

$$\left.\begin{array}{l} \text{Si } \ c = 0\ \rightarrow\ (\ f(x)\ ) = \{0\} \\ \text{Si } \ c \neq 0\ \rightarrow\ (\ f(x)\ ) = \ A \end{array}\right\} \Rightarrow \text{ en cualquier caso, } (\ f(x)\ ) \text{ es ideal primo.}$$

b) Veamos que $(\ f(x)\ )$ es ideal maximal si y sólo si $f(x)$ es irreducible no constante.
$[\ \Rightarrow\ ]$ Si $(\ f(x)\ )$ es un ideal maximal, como tiene que ser un ideal propio, es inmediato que $f(x)$ no es constante. Además, como en general todo ideal maximal de un anillo es primo, se tiene que $(\ f(x)\ )$ es ideal primo. Del apartado a) sabemos que ello implica que $f(x)$ es irreducible sobre F.
$[\ \Leftarrow\ ]$ Si $f(x)$ es irreducible y no es constante, sea J un ideal propio de $F[x]$ tal que $J \supset (\ f(x)\ )$. Suponiendo que $I \neq J$, existe $g(x) \in J$ tal que $g(x) \notin (\ f(x)\ )$. Entonces

$$\left.\begin{array}{l} f(x)\ \not| g(x) \\ f(x)\ irred. \end{array}\right\} \exists p(x), q(x) \in F[x]/1 = f(x)p(x)+g(x)q(x) \Rightarrow 1 \in J \Rightarrow J = A. \text{Absurdo. } \clubsuit$$

Ex. 327 *Hallar un ideal primo de $\mathbf{Q}[x, y]$ que no sea maximal.*

$\equiv$

Sea $I := (\ x\ )$. Veamos que I es un ideal primo. Si $f(x,y), g(x,y) \in \mathbf{Q}[x,y]$ son tales que $f(x,y)g(x,y) \in (\ x\ )$, entonces, como $(\ x\ ) = \{h(x,y) \in \mathbf{Q}[x,y] \quad h(0,y) = 0\}$, tenemos que

$$0 = f(0,y)g(0,y) \rightarrow \left\{ \begin{array}{ccc} f(0,y) = 0 & \rightarrow & f(x,y) \in (\ x\ ) \\ \acute{o} & \rightarrow & \acute{o} \\ g(0,y) = 0 & \rightarrow & g(x,y) \in (\ x\ ). \end{array} \right.$$

Claramente, $(\ x\ )$ no es maximal, ya que $(\ x\ ) \subset (\ x,y\ )$, que es un ideal propio de $\mathbf{Q}[x,y]$. ♣

Ex. 328 *Dados un anillo unitario conmutativo A y un ideal I, demostrar que existe una correspondencia inyectiva entre la familia de ideales del anillo cociente A/I y la familia de ideales de A que contienen I.*

$\equiv$

Sea trata de definir una aplicación inyectiva entre dos familias de conjuntos. Por comodidad, llamamos

$$\begin{array}{ll} \mathcal{I}_{A/I} & \equiv \text{ Familia de ideales de } A/I \\ \mathcal{I}_A^I & \equiv \text{ Familia de ideales de A que contienen } I. \end{array}$$

Definimos

$$\begin{array}{rcl} \psi & : & \mathcal{I}_{A/I} \longrightarrow \mathcal{I}_A^I \\ & & \tilde{J} \rightarrow \psi(\tilde{J}) := \{x \in A \ : \ x + I \in \tilde{J}\}. \end{array}$$

ψ bien definida: Si $\tilde{J} \in \mathcal{I}_{A/I}$, hay que ver que $\psi(\tilde{J})$ es un ideal de A conteniendo I. Así

$$x,y \in \psi(\tilde{J}),\ a \in A \rightarrow \left\{ \begin{array}{l} (x-y) + I = (x+I) - (y+I) \in \tilde{J} \rightarrow x - y \in \psi(\tilde{J}) \\ (ax) + I = (a+I)(x+I) \in \tilde{J} \rightarrow ax \in \psi(\tilde{J}). \end{array} \right.$$

Si $x \in I$, es obvio que $x + I = I \in \tilde{J}$, ya que I es el cero del anillo cociente A/I. Por tanto, $x \in \psi(\tilde{J})$.

ψ inyectiva: Sean $\widetilde{J_1}, \widetilde{J_2} \in \mathcal{I}_{A/I}$ tales que $\psi(\widetilde{J_1}) = \psi(\widetilde{J_2})$. Entonces

$$\left. \begin{array}{l} x + I \in \widetilde{J_1} \rightarrow x \in \psi(\widetilde{J_1}) = \psi(\widetilde{J_2}) \rightarrow x + I \in \widetilde{J_2} \Rightarrow \widetilde{J_1} \subset \widetilde{J_2} \\ x + I \in \widetilde{J_2} \rightarrow x \in \psi(\widetilde{J_2}) = \psi(\widetilde{J_1}) \rightarrow x + I \in \widetilde{J_1} \Rightarrow \widetilde{J_2} \subset \widetilde{J_1} \end{array} \right\} \Rightarrow \widetilde{J_1} = \widetilde{J_2}. \ \clubsuit$$

Ex. 329 *Dos ideales I, J del anillo unitario conmutativo A se dicen primos relativos siempre que $I + J = A$. Demostrar que, si I, J son ideales primos relativos, entonces $A/IJ \cong A/I \times A/J$.*

$\equiv$

Definimos

$$\begin{array}{rcl} \psi & : & A \longrightarrow A/I \times A/J \\ & & x \rightarrow \psi(x) := (x + I, x + J). \end{array}$$

ψ homomorfismo de anillos: Dados $x, y \imath A$

$$\psi(x+y) = (x+y+I, x+y+J) = (x+I, x+J) + (y+I, y+J) = \psi(x) + \psi(y)$$
$$\psi(xy) = (xy+I, xy+J) = (x+I, x+J)(y+I, y+J) = \psi(x)\psi(y).$$

ψ sobre: Dado el par $(a+I, b+J) \in A/I \times A/J$, como $A = I+J$, existen $x \in I$, $y \in J$ tales que $a - b = x + y$. Entonces

$$(a+I, b+J) = (b+x+y+I, b+J) = (b+y+I, b+y+J) = \psi(b+y).$$

$Ker(\psi) = IJ$: Observemos que, de un problema resuelto anteriormente, al ser $A = I+J$, se deduce que $I \cap J = IJ$. Así

$$x \in Ker(\psi) \leftrightarrow (I, I) = \psi(x) = x+I, x+J) \leftrightarrow x \in I \cap J = IJ.$$

Por tanto

$$A/IJ = A/Ker(\psi) \cong \psi(A) = A/I \times A/J. \clubsuit$$

4.3. Divisibilidad en un anillo

Ex. 330 *Sea* $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{3}}$. *Demostrar que* $\mathbf{Z}(\omega)$ *es un dominio euclídeo para* $\delta(a+b\omega) = a^2 - ab + b^2$.

$\equiv$

Primero recordemos que $\mathbf{Z}(\omega)$ representa al menor anillo conteniendo $\mathbf{Z} \cup \{\omega\}$. También recordemos que un dominio euclídeo es un dominio de integridad D provisto de una aplicación $\delta : D^* = D \setminus \{0\} \to \mathbf{N} \cup \{0\}$, llamada norma (de anillos) que ha de cumplir:

1) $\forall a, b \in D^*$, $\delta(ab) \geq \delta(a)$.

2) $\forall a \in D$, $\forall b \in D^*$, $\exists q, r \in D$ tales que: $a = bq + r$, y, $\begin{cases} r = 0 \\ \acute{o} \\ \delta(r) < \delta(b). \end{cases}$

Por tanto, hay que ver que $\delta(a+b\omega) = a^2 - ab + b^2$, $a + b\omega \in \mathbf{Z}(\omega)^*$, es una norma de anillos. Veamos la primera condición: Sean $a + b\omega, c + d\omega \in \mathbf{Z}(\omega)^*$

$$\delta[(a+b\omega)(c+d\omega)] \overset{(1+\omega+\omega^2=0)}{=} \delta[(ac-bd) + (ad+bc-bd)\omega]$$
$$= (ac-bd)^2 - (ac-bd)(ad+bc-bd) + (ad+bc-bd)^2$$
$$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 + abcd - a^2cd - abc^2 - abd^2 - b^2cd.$$

Por otra parte

$$\delta(a+b\omega)\delta(c+d\omega) = (a^2 - ab + b^2)(c^2 - cd + d^2)$$
$$= a^2c^2 - a^2cd + a^2d^2 - abc^2 + abcd - abd^2 + b^2c^2 - b^2cd + b^2d^2.$$

Así pues hemos demostrado la igualdad

$$\delta[(a+b\omega)(c+d\omega)] = \delta(a+b\omega) \cdot \delta(c+d\omega).$$

Por tanto, para obtener la primera desigualdad simplemente hay que probar que $\delta(c+d\omega) \geq 1$, lo que equivale a que $\delta(c+d\omega) \neq 0$:

$$0 = \delta(c+d\omega) = c^2-cd+d^2 \Rightarrow c^2+d^2 = cd \overset{(ver\ Nota)}{\leq} \frac{c^2+d^2}{2} \Rightarrow c = d = 0, \ Absurdo.$$

Veamos ahora la segunda condición: Si $\alpha := a+b\omega$, $\beta := c+d\omega \in \mathbf{Z}(\omega)$, con $\beta \neq 0$, como $\frac{\alpha}{\beta} \in \mathbf{Q}(\omega)$, existen $u, v \in Q$ tales que $\frac{\alpha}{\beta} = u + v\omega$. Sean $p, q \in \mathbf{Z}$ tales que $\mid u-p \mid \leq \frac{1}{2}$, $\mid v-q \mid \leq \frac{1}{2}$ (p, q son los enteros más cercanos a u, v, respectivamente). Ahora, sean $\gamma := p+q\omega \in \mathbf{Z}(\omega)$ y $\rho := \alpha - \beta\gamma \in \mathbf{Z}(\omega)$. Como $\alpha = \beta\gamma + \rho$, todo consiste en ver que, si $\rho \neq 0$, entonces $\delta(\rho) < \delta(\beta)$:

$$\delta(\rho) = \delta(\alpha - \beta\gamma) = \delta[\beta(\frac{\alpha}{\beta} - \gamma] = \delta(\beta)\delta(\frac{\alpha}{\beta} - \gamma),$$

por lo que es suficiente con ver que $\delta(\frac{\alpha}{\beta} - \gamma) < 1$.

$$\delta(\frac{\alpha}{\beta}-\gamma) = \delta[(u-p)+(v-q)\omega] = (u-p)^2-(u-p)(v-q)+(v-q)^2 \leq \frac{3}{2}[(u-p)^2+(v-q)^2]$$

$$\leq \frac{3}{2}(\frac{1}{4}+\frac{1}{4}) = \frac{3}{4} < 1.\clubsuit$$

Nota 35 En algunas desigualdades del ejercicio previo hemos usado la siguiente desigualdad, que es muy frecuente e importante: $\forall x, y \in \mathbf{R}$, $x^2+y^2 \geq 2 \mid xy \mid$. Demostrémosla:

$$0 \leq (\mid x \mid - \mid y \mid)^2 = x^2+y^2-2 \mid xy \mid \Rightarrow x^2+y^2 \geq 2 \mid xy \mid .$$

Como consecuencia

$$\text{máx}\{-xy, xy\} \leq \mid xy \mid \leq \frac{x^2+y^2}{2}.$$

Ex. 331 *Sea D un dominio euclídeo. Sean $a, b \in D$ no simultáneamente nulos. Un elemento $d \in D$ se dice que es un máximo común divisor (m.c.d.) de a, b cuando cumple*

$$d \mid a \ \ (i.e., \exists x \in D / \ dx = a), \qquad d \mid b, \quad c \in D \left\{ \begin{array}{c} c \mid a \\ c \mid b \end{array} \right\} \rightarrow \ c \mid d.$$

Demostrar que, dados $a, b \in D$ no simultáneamente nulos, existen $r, s \in D$ tales que $ra+sb$ es un m.c.d. de a, b.

≡

Consideremos el ideal $I := (\ a, b\ )$, es decir, I es el menor ideal que contiene a, b. Sabemos que $I = \{ra+sb \ : \ r, s \in D\}$. Como D es dominio euclídeo, debemos saber (Teoría de Anillos) que D es un dominio de ideales principales. Por tanto, existe $d \in D$ tal que $I = (\ d\ )$. Entonces

$$\left.\begin{array}{l} a \in (\ d\ ) \ \rightarrow \ d \mid a \\ b \in (\ d\ ) \ \rightarrow \ d \mid b \\ Si\ c \in D \ / \ c \mid a, \ c \mid b \ \rightarrow \ a, b \in (\ c\ ) \ \rightarrow \ (\ d\ ) = I \subset (\ c\ ) \rightarrow \ c \mid d. \end{array}\right\} d \text{ es m.c.d. de } a, b.$$

Finalmente, como $d \in I$, de la descripción de I dada inicialmente, existen $r, s \in D$ tales que $d = ra+sb$. $\clubsuit$

Ex. 332 *Demostrar que* $\mathbf{Z}(\sqrt{-3})$ *no es un dominio euclídeo, ni tampoco un dominio de factorización única.*

≡

Para resolver est ejercicio necesitamos recordar dos definiciones y dos resultados fundamentales. En un dominio de integridad D un elemento $x \in D,\ x \neq 0$, es irreducible, o primo siempre que, si existen $a, b \in D$ tales que $x = ab$, ello obliga a que a ó b ha de ser unitario (inversible). Entonces, el dominio D se dice que es un dominio de factorización única (DFU) siempre que todo elemento no nulo de D se puede expresar de manera única, salvo producto por unitarios, como producto de elementos irreducibles. Los siguientes resultados son de gran importancia:

1) Todo dominio de ideales principales (DIP) es un dominio de factorización única, i.e. $DIP \Rightarrow DFU$.
2) Todo dominio euclídeo (DE) es un dominio de factorización única, i.e. $DE \Rightarrow DFU$.

Volviendo al ejercicio, "matamos dos pájaros de un tiro"viendo que $\mathbf{Z}(\sqrt{-3})$ no es DFU. Para ello, observemos que

$$4 = \left\{ \begin{array}{l} 2^2 \\ (1+\sqrt{-3})(1-\sqrt{-3}) \end{array} \right\} \Rightarrow \text{ 4 admite factorizaciones irreducibles distintas,}$$

ya que $2, 1+\sqrt{-3}, 1-\sqrt{-3}$ son irreducibles en $\mathbf{Z}(\sqrt{-3})$. ♣

Ex. 333 *En un dominio euclídeo* D *con norma* δ*, demostrar que:* $u \in D$ *es unitario si y sólo si* $\delta(u) = \delta(1)$.

≡

[$\Rightarrow$] Sea $u \in D$ un elemento unitario. Entonces existe $u^{-1} \in D$ tal que $uu^{-1} = 1$. Observemos que

$$\delta(u) \leq \delta(u \cdot u^{-1}) = \delta(1) \leq \delta(1 \cdot u) = \delta(u).$$

[$\Leftarrow$] Sea $u \in D$ tal que $\delta(u) = \delta(1)$. Antes ya lo hemos demostrado, aunque no lo hemos dicho, notar que $\forall x \in D^*,\ \delta(1) \leq \delta(x)$, ya que $\delta(x) = \delta(1 \cdot x) \geq \delta(1)$. Así, de la segunda condición que cumple δ, existen $q, r \in D$ tales que $1 = uq + r$, con $r = 0$, ó, $\delta(r) < \delta(1)$. De lo visto antes, es obligatorio que $r = 0$, de donde $1 = uq$, i.e., u es unitario. ♣

Ex. 334 *Demostrar que, en un dominio de integridad, dos elementos son asociados, si y sólo si general el mismo ideal principal.*

≡

Dos elementos a, b de un anillo unitario conmutativo A son asociados siempre que existe algún elemento unitario $u \in A$ tal que $a = bu$.

[$\Rightarrow$] Sean a, b elementos asociados del dominio de integridad D. Sea $u \in D$ un elemento unbitario tal que $a = bu$. Entonces

$$\left. \begin{array}{l} a \in (\ b\ ) \rightarrow (\ a\ ) \subset (\ b\ ) \\ b = au^{-1} \rightarrow b \in (\ a\ ) \rightarrow (\ b\ ) \subset (\ a\ ) \end{array} \right\} \Rightarrow (\ a\ ) = (\ b\ ).$$

[$\Leftarrow$] Si (a) = (b), existen $x, y \in D$ tales que $a = bx$, $b = ay$. Por tanto

$$a = axy \ \rightarrow \ (xy-1)a = 0 \ \rightarrow \begin{cases} \text{Si } a = 0 \rightarrow \ b = 0 \text{ a, b son asociados} \\ \text{Si } xy = 1 \rightarrow \ x, y \text{ unitarios} \rightarrow \text{ a, b son asociados. } \clubsuit \end{cases}$$

Ex. 335 *Demostrar que todo elemento asociado de un primo es primo*

≡

Recordemos primero que, en un anillo unitario conmutativo A un elemento $p \in A \setminus \{0\}$ es primo siempre que, si $p = x_1 x_2 ... x_n$, $x_1, ..., x_n \in A$, entonces alguno de los factores $x_1, ..., x_n$ ha de ser unitario.

Sea $p \in A$ un elemento primo del anillo unitario conmutativo A. Sea $q \in A$ un asociado de p. Así, existe un elemento unitario $u \in A$ de modo que $q = up$. Si q no es primo, entonces $q = a_1 a_2 ... a_n$, donde cada a_i, $1 \leq i \leq n$, no es unitario. Así $p = u^{-1} a_1 a_2 ... a_n$. Llamando $b_1 := u^{-1} a_1$, $b_2 := a_2, ..., b_n := a_n$, tenemos que $p = b_1 b_2 ... b_n$. Ahora bien, $b_2, ..., b_n$ no son unitarios y b_1 tampoco es unitario (de serlo, existiría $c \in D$ tal que $1 = b_1 c = u^{-1} a_1$, lo que implicaría que a_1 fuese unitario). Ello es absurdo, ya que p es primo. $\clubsuit$

Ex. 336 *De los números* $3, 5, 7, 11, 13, 17, 19$, *indicar cuáles son primos en* $\mathbf{Z}(\sqrt{2})$.

≡

Veamos que 3 es primo en el dominio euclídeo $\mathbf{Z}(\sqrt{2})$ (la norma es $\delta(a + b\sqrt{2}) = \mid a^2 - 2b^2 \mid$). Si $3 = \alpha\beta$, $\alpha, \beta \in \mathbf{Z}(\sqrt{2})$, entonces

$$9 = \delta(3) = \delta(\alpha)\delta(\beta) \ \rightarrow \ \delta(\alpha) \in \{1, 3, 9\}.$$

Supongamos que $\alpha = x + y\sqrt{2}$.

$$3 = \delta(\alpha) = \mid x^2 - 2y^2 \mid \text{ es irresoluble en } \mathbf{Z} \ \rightarrow \ \delta(\alpha) \in \{1, 9\}.$$

Ello implica entonces que, o bien α, o bien β, es unitario, es decir 3 es primo en $\mathbf{Z}(\sqrt{2})$.

Análogamente se vé que $5, 11, 13$ y 19 también son primos en $\mathbf{Z}(\sqrt{2})$. Sin embargo,

$$\left.\begin{array}{l} 7 = (3+\sqrt{2})(3-\sqrt{2}) \\ 3+\sqrt{2}, 3-\sqrt{2} \text{ no unitarios} \end{array}\right\} \ \rightarrow \ 7 \text{ no es primo en } \mathbf{Z}(\sqrt{2})$$

$$\left.\begin{array}{l} 17 = (5+2\sqrt{2})(5-2\sqrt{2}) \\ 5+2\sqrt{2}, 5-2\sqrt{2} \text{ no unitarios} \end{array}\right\} \ \rightarrow \ 17 \text{ no es primo en } \mathbf{Z}(\sqrt{2}). \ \clubsuit$$

Ex. 337 *Sea A un anillo unitario conmutativo. Dados $a, b \in A$, un elemento $m \in A$ es un mínimo común múltiplo de a, b siempre que cumple*

1) $a \mid m$, $b \mid m$.

2) Si $c \in A$ es tal que $a \mid c$, $b \mid c$, entonces $m \mid c$. Demostrar que m es un mínimo común múltiplo de a, b si y sólo si (m) = (a) $\cap$ (b).

$\equiv$

[$\Rightarrow$] Sea m un mínimo común múltiplo de a, b. Entonces

$$\left.\begin{array}{l} a \mid m \rightarrow\ m \in (\ a\ ) \\ b \mid m \rightarrow\ m \in (\ b\ ) \end{array}\right\} \Rightarrow\ m \in (\ a\ ) \cap (\ b\ ) \Rightarrow\ (\ m\ ) \subset (\ a\ ) \cap (\ b\ )$$
$$\forall x \in (\ a\ ) \cap (\ b\ )\ \rightarrow\ a \mid x,\ b \mid x\ \rightarrow\ m \mid x\ \rightarrow\ x \in (\ m\ ), i.e., (\ a\ ) \cap (\ b\ ) \subset (\ m\ ).$$

[$\Leftarrow$] Si $(\ m\ ) = (\ a\ ) \cap (\ b\ )$. Entonces, como $m \in (\ a\ ) \cap (\ b\ )$, se tiene que $a \mid m$, $b \mid m$. Además, si $c \in A$ es tal que $a \mid c$, $b \mid c$, entonces $c \in (\ a\ ) \cap (\ b\ ) = (\ m\ )$, lo que implica que $m \mid c$. Es decir, m es un mínimo común múltiplo de a, b. ♣

Ex. 338 *Sea D un dominio de ideales principales. Dados $a, b \in D$, sean d y m un máximo común divisor y un mínimo común múltiplo de a, b, respectivamente. Demostrar que dm y ab son asociados.*

$\equiv$

Por las definiciones correspondientes, sabemos que

$$(\ d\ ) = (\ a\ ) + (\ b\ ), \qquad (\ m\ ) = (\ a\ ) \cap (\ b\ ).$$

Así, existen $p, q, r, s \in D$ tales que

$$d = pa + qb, \quad m = ra = sb.$$

Entonces

$$dm = pra^2 + qrab = psab + qrab = (ps + qr)ab\ \rightarrow\ dm \in (\ ab\ ).$$

Recíprocamente, sean $a', b' \in D$ tales que $a = da'$, $b = db'$. Entonces

$$ab = da'b = adb'\ \rightarrow\ d(a'b - ab') = 0 \overset{(d \neq 0,\ sino\ a=b=0)}{\rightarrow} a'b - ab' = 0.$$

Así

$$\left.\begin{array}{l} a \mid a'b \\ b \mid ab' \end{array}\right\} \overset{(m\ es\ m.c.m.)}{\rightarrow} m \mid a'b\ \rightarrow\ \exists u \in D\ /\ mu = a'b.$$

Consecuentemente

$$dmu = da'b = ab\ \rightarrow\ ab \in (\ dm\ ).\ \clubsuit$$

Ex. 339 *Sea p un número primo y $n \in \mathbf{N}$. Demostrar que $\mathbf{Z}_{p^n}$ es un dominio de factorización única.*

$\equiv$

Suponemos que $n \geq 2$, ya que, de ser $n = 1$, se tendría que $\mathbf{Z}_p$ es un cuerpo y, como todo elemento no nulo es unitario, es evidente que es un DFU.

Necesitamos previamente algunos resultados de apoyo.

Lema 12 *$\overline{a} \in \mathbf{Z}_{p^n}$ es unitario si y sólo si $p \not| a$.*

$\equiv$

$[\Rightarrow]$ Supongamos que $\overline{a} \in \mathbf{Z}_{p^n}$ es unitario. Entonces existe $\overline{b} \in \mathbf{Z}_{p^n}$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$. Ello implica que, para un entero q, $1 - ab = qp^n$. Es decir

$$1 = ab + qp^n \overset{(Bezout)}{\rightarrow} mcd(a, p^n) = 1 \rightarrow mcd(a, p) = 1 \rightarrow p \not| a.$$

$[\Leftarrow]$

$p \not| a \rightarrow mcd(a, p) = 1 \rightarrow mcd(a, p^n) = 1 \rightarrow \exists b, c \in \mathbf{Z} \,/\, 1 = ba + cp^n \overset{(en\ \mathbf{Z}_{p^n})}{\rightarrow} \overline{a} \cdot \overline{b} = \overline{1}$. •

Lema 13 *$\overline{a}$ es un primo propio de $\mathbf{Z}_{p^n}$ si y sólo si $\overline{a}$ es un asociado de $\overline{p}$.*

$\equiv$

$[\Rightarrow]$ Supongamos que $\overline{a}$ es un primo propio de $\mathbf{Z}_{p^n}$. Entonces $\overline{a}$ no es unitario. Del lema anterior, $p \mid a$. Así, existe $b \in \mathbf{Z}$ tal que $a = pb$. Entonces

$$\left.\begin{array}{l} \overline{p}\,\overline{b} = \overline{a} \text{ primo} \\ \overline{p} \text{ no unitario} \end{array}\right\} \Rightarrow \overline{b} \text{ es unitario} \Rightarrow \overline{a} \text{ es asociado de } \overline{p}.$$

$[\Leftarrow]$ Si $\overline{a}$ es un asociado de $\overline{p}$ en $\mathbf{Z}_{p^n}$, para ver que $\overline{a}$ es primo, de un ejercicio anterior, todo consiste en ver que $\overline{p}$ es primo en $\mathbf{Z}_{p^n}$. Supongamos que $\overline{p} = \overline{a}\overline{b}$. Entonces existe $q \in \mathbf{Z}$ tal que $p - ab = qp^n$. Ello implica que $p \mid ab$. Supongamos que $p \mid a$ (se haría de modo similar si $p \mid b$). Sea $a' := \frac{a}{p} \in \mathbf{Z}$. Entonces

$$1 = a'b + qp^{n-1} \rightarrow mcd(b, p) = 1 \rightarrow p \not| b \overset{(lema\ previo)}{\rightarrow} \overline{b} \text{ es unitario.}$$

Por tanto, $\overline{p}$ no admite factorización propia, i.e., $\overline{p}$ es primo. •

Volviendo al ejercicio, Sea $\overline{a}$ un elemento propio de $\mathbf{Z}_{p^n}$. Del primero de los lemas, sabemos que $p \mid a$. Sea $m := \max\{k \in \mathbf{N} : p^k \mid a\}$. Sea $b \in \mathbf{Z}$ tal que $a = bp^m$. Así, en $\mathbf{Z}_{p^n}$, tenemos que $\overline{a} = \overline{b} \cdot \overline{p}^m$. Puesto que $p^{m+1} \not| a$, se tiene que $p \not| b$, por lo que, del primer lema de nuevo, $\overline{b}$ es unitario. Por tanto, del segundo lema, $\overline{a} = \overline{p}^{m-1}(\overline{b}\overline{p})$ es una factorización en primos propios.

Finalmente, sea $\overline{a} = \overline{q_1 q_2 ... q_k}$ otra factorización de $\overline{a}$ en primos propios. Aplicando el segundo lema, para $i = 1, 2, ..., k$, existe un unitario $\overline{u_i}$ tal que $\overline{q_i} = \overline{pu_i}$. Así

$$\overline{a} = \overline{p}^k(\overline{u_1 u_2 ... u_k}) \overset{(\overline{u} := \overline{u_2} ... \overline{u_k})}{=} \overline{p}^k \overline{u}.$$

Consecuentemente, de lo hecho antes, tenemos que

$$\overline{a} = \overline{p}^m \overline{b} = \overline{p}^k \overline{u}.$$

Así pues, todo se reduce a ver que $m = k$. Suponiendo que $m < k$ (si $m > k$, se contradice la definición de m), tenemos

$$\overline{0} = \overline{p}^m(\overline{b} - \overline{p}^{k-m}\overline{u})$$

$$\rightarrow \exists q \in \mathbf{Z} \,/\, p^m(b - p^{k-m}u) = qp^n \rightarrow b = p^{k-m}u + qp^{n-m} = p^{k-m}(u + p^{n-k}).$$

Como $k - m \geq 1$, se deduce que $p \mid b$, lo que supone una contradicción. ♣

Ex. 340 *Demostrar que un anillo cociente de un anillo de factorización única no tiene porqué ser anillo de factorización úica.*

≡

Este ejercicio se resuelve aportando un contraejemplo adecuado.

Contraex. Sabemos que $\mathbf{Z}$ es un DFU, sin embargo, vamos a demostrar que el anillo cociente $\mathbf{Z}_6 = \mathbf{Z}/(\ 6\ )$ no es de factorización única. Para ello, basta con ver que $\mathbf{Z}_6$ no tiene elementos primos propios, aunque sí tiene elementos propios, con lo cual no se cumple la primera condición de ser anillo de factorización única.

$\mathbf{Z}_6 = \{\ \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$
Elementos unitarios : $\overline{1},\ \overline{5} \qquad [\overline{5}\cdot\overline{5} = \overline{1}]$

Elementos propios (no nulos, ni unitarios) : $\overline{2},\ \overline{3},\ \overline{4} \rightarrow \begin{cases} \overline{2} = \overline{2}\cdot\overline{2}\cdot\overline{2} \rightarrow \overline{2} \text{ no es primo} \\ \overline{3} = \overline{3}\cdot\overline{3} \rightarrow \overline{3} \text{ no es primo} \\ \overline{4} = \overline{2}\cdot\overline{2} \rightarrow \overline{4} \text{ no es primo.} \end{cases}$

Como $\mathbf{Z}_6$ no tiene primos propios, queda claro que ninguno de los elementos propios $(\overline{2}, \overline{3}, \overline{4})$ puede expresarse como producto de primos propios. ♣

Ex. 341 *Demostrar que, en un dominio de ideales principales, todo idel primo propio es maximal.*

≡

Observemos que este resultado nos dice que, en un DIP, los ideales maximales coinciden con los primos (lo que sucede, por ejemplo, en $\mathbf{Z}$).

Sea I un ideal primo propio del DIP D. Sea J un ideal de D tal que $J \supset I$. Al ser D un DIP, existen $a, b \in D$ tales que $I = (\ a\ )$, $J = (\ b\ )$. Entonces

$$I \subset J \rightarrow \exists c \in D / a = bc \in I \overset{(I \text{ primo})}{\Rightarrow} \begin{cases} b \in I = (\ a\ ) \\ \rightarrow\ J = (\ b\ ) = (\ a\ ) = I \\ \quad \acute{o} \\ c \in I = (\ a\ ) \\ \rightarrow \exists c \in D / c = ad \rightarrow a = abd; a(1 - bd) = 0. \end{cases}$$

Siguiendo de la segunda posibilidad, como D es un dominio de integridad y $a \neq 0$ (al ser I propio), se desprende que $bd = 1$. Esto nos dice que b es un unitario de D, por lo que $J = (\ b\ ) = D$. Ello prueba que I es maximal. ♣

Ex. 342 *Utilizando como norma en* $\mathbf{Z}(\sqrt{-5})$ *la función* $\delta(a + b\sqrt{-5}) = a^2 + 5b^2$

a) Determinar los elementos unitarios de $\mathbf{Z}(\sqrt{-5})$.

b) Demostrar que $2, 3,$ *y* $1 \pm \sqrt{-5}$ *son primos propios.*

c) Demostrar que $\mathbf{Z}(\sqrt{-5})$ *no es anillo de factorización única.*

≡

a) Veamos que los únicos unitarios de $\mathbf{Z}(\sqrt{-5})$ son ± 1:

$a + b\sqrt{-5}$ unitario $\rightarrow\ 1 = \delta(a + b\sqrt{-5}) = a^2 + 5b^2 \rightarrow\ b = 0$ (si $b \neq 0 \rightarrow\ a^2 + 5b^2 \geq 5 > 1$)

$$\Rightarrow\ a^2 = 1 \rightarrow\ a + b\sqrt{-5} = \pm 1.$$

b)

$$2 = (a+b\sqrt{-5})(c+d\sqrt{-5}) \rightarrow\ 4 = \delta(2) = \delta(a+b\sqrt{-5})\delta(c+d\sqrt{-5}) = (a^2+5b^2)(c^2+5d^2)$$

$$\rightarrow \left\{ \begin{array}{l} a^2+5b^2 \mid 4 \\ c^2+5d^2 \mid 4 \end{array} \right\} \Rightarrow\ b = d = 0\ \rightarrow\ \left\{ \begin{array}{l} a+b\sqrt{-5} = a \\ c+d\sqrt{-5} = c \end{array} \right\} \Rightarrow\ 4 = (ac)^2$$

$$\rightarrow\ ac = \pm 2 \rightarrow \left\{ \begin{array}{l} a \in \{\pm 1\} \\ c \in \{\pm 1\} \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} a+b\sqrt{-5} \text{ es unitario} \\ c+d\sqrt{-5} \text{ es unitario.} \end{array} \right.$$

Por tanto, 2 es un primo propio de $\mathbf{Z}(\sqrt{-5})$. Hacemos algo similar para 3

$$3 = (a+b\sqrt{-5})(c+d\sqrt{-5}) \rightarrow\ 9 = \delta(3) = \delta(a+b\sqrt{-5})\delta(c+d\sqrt{-5}) = (a^2+5b^2)(c^2+5d^2)$$

$$\rightarrow \left\{ \begin{array}{l} a^2+5b^2 \mid 9 \\ c^2+5d^2 \mid 9 \end{array} \right\} \Rightarrow\ b = d = 0\ \rightarrow\ \left\{ \begin{array}{l} a+b\sqrt{-5} = a = \pm 1 \\ c+d\sqrt{-5} = c = \pm 1. \end{array} \right.$$

Finalmente lo vemos para $1 \pm \sqrt{-5}$

$$1 \pm \sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5})$$

$$\rightarrow\ 6 = \delta(1 \pm \sqrt{-5}) = \delta(a + b\sqrt{-5})\delta(c + d\sqrt{-5}) = (a^2 + 5b^2)(c^2 + 5d^2)$$

$$\rightarrow \left\{ \begin{array}{l} a^2+5b^2 \mid 6 \\ c^2+5d^2 \mid 6 \end{array} \right\} \Rightarrow\ b = d = 0\ \rightarrow\ \left\{ \begin{array}{l} a+b\sqrt{-5} = a = \pm 1 \\ c+d\sqrt{-5} = c = \pm 1. \end{array} \right.$$

c) Para ver que $\mathbf{Z}(\sqrt{-5})$ no es un DFU, basta fijarse en que

$$6\ =\ \left\{ \begin{array}{l} 2 \cdot 3 \\ (1+\sqrt{-5})(1-\sqrt{-5}), \end{array} \right.$$

que nos indica que 6 tiene dos factorizaciones distintas en primos propios. ♣

Ex. 343 *Sea* $I = \{a + b\sqrt{-5} \in \mathbf{Z}(\sqrt{-5}) : a \equiv b\ (mod,2)\}$.

a) Demostrar que I es un ideal maximal de $\mathbf{Z}(\sqrt{-5})$.

b) Demostrar que $I = (\ 2,\ 1+\sqrt{-5}\ )$.

c) Demostrar que $I^2 = (\ 2\ )$.

d) Demostrar que I no es un ideal principal.

≡

a) Dados $a + b\sqrt{-5}, c + d\sqrt{-5} \in I$, $x + y\sqrt{-5} \in \mathbf{Z}(\sqrt{-5})$. Sabemos que $a - b = 2p$, $c - d = 2q$. Así

$$(a + b\sqrt{-5}) - (c + d\sqrt{-5}) = (a - c) + (b - d)\sqrt{-5}$$
$$\rightarrow\ (a - c) - (b - d) = 2(p - q)$$

$$(x + y\sqrt{-5})(a + b\sqrt{-5}) = (xa - 5yb) + (xb + ya)\sqrt{-5}$$
$$\rightarrow\ (xa - 5yb) - (xb + ya) = 2(xp - py - 3by)$$

Por tanto, I es un ideal de $\mathbf{Z}(\sqrt{-5})$. Veamos que I es maximal: Sea J un ideal de $\mathbf{Z}(\sqrt{-5})$ tal que $J \supset I$. Suponinedo que $J \neq I$, sea $a+b\sqrt{-5} \in J$ tal que $a \not\equiv b\ (mod,2)$. Entonces existe $p \in \mathbf{Z}$ tal que $a-b = 2p+1$. Así, $a+1+b\sqrt{-5} \in I$. Pero éso implica que

$$1 \;=\; (a+1+b\sqrt{-5}) - (a+b\sqrt{-5}) \;\in\; J \;\Rightarrow\; J \;=\; \mathbf{Z}(\sqrt{-5}).$$

b) Obviamente $2,\ 1+\sqrt{-5} \in I$, por lo tanto $(\ 2,\ 1+\sqrt{-5}\ ) \subset I$. Recíprocamente

$$\forall a+b\sqrt{-5} \in I,\ \ \exists p \in \mathbf{Z}\ /\ a-b = 2p \rightarrow\ a+b\sqrt{-5} = 2p+b+b\sqrt{-5} = p\cdot 2 + b(1+\sqrt{5}).$$

Es decir, $a+b\sqrt{-5} \in (\ 2,\ 1+\sqrt{-5}\ )$.
c) Como $I \;=\; (\ 2\ ) + (\ 1+\sqrt{-5}\ )$, aprovechando la propiedad distributiva de los ideales demostrada en ejercicios anteriores

$$I^2 = (\ 2\ )^2 + (\ 1+\sqrt{-5}\ )^2 + (\ 2\ )(\ 1+\sqrt{-5}\ )$$

$$= (\ 4\ ) + (\ -4+2\sqrt{-5}\ ) + (\ 2+2\sqrt{-5}\ ) \overset{(obviamente)}{\subset} (\ 2\ ).$$

Recíprocamene

$$2 \;=\; -4-(-4+2\sqrt{-5})+(2+2\sqrt{-5}) \;\rightarrow\; 2 \;\in\; I^2 \;\rightarrow\; (\ 2\ ) \;\subset\; I^2.$$

d) Suponiendo que I fuese principal, existe un $\alpha \in \mathbf{Z}(\sqrt{-5})$ tal que $I = (\ \alpha\ )$. Como $2 \in I = (\ \alpha\ )$, existe $\beta \in \mathbf{Z}(\sqrt{-5})$ tal que $2 = \alpha\beta$. Pero, al ser 2 primo en $\mathbf{Z}(\sqrt{-5})$, se tiene que α es unitario, ó β es unitario.

α unitario $\rightarrow\ I = \mathbf{Z}(\sqrt{-5})$, absurdo
β unitario $\rightarrow \alpha = 2\beta^{-1} \rightarrow\ I = (\ \alpha\ ) = (\ 2\ ) \rightarrow\ 1+\sqrt{-5} \in (\ 2\ )$, absurdo.

Así pues, I no es ideal principal. ♣

4.4. Homomorfismos de anillos

Ex. 344 *Si $\varphi\ :\ A \rightarrow\ A'$ es un hmomorfismo de anillos, demostrar que*

$$Ker(\varphi) \;=\; \{a \in A\ :\ \ f(a) = 0\ \}$$

es un ideal de A.

≡

Verificando las dos condiciones de idealidad:
1) Si $a, b \in Ker(\varphi)$, entonces

$$\varphi(a-b) \;=\; \varphi(a) - \varphi(b) \;=\; 0-0 \;=\; 0 \;\rightarrow\; a-b \;\in\; Ker(\varphi).$$

2) Si $x \in Ker(\varphi)$ y $a \in A$ entonces

$$\varphi(ax) \;=\; \varphi(a)\varphi(x) \;=\; \varphi(a)\cdot 0 \;=\; 0 \;\rightarrow\; ax \;\in\; Ker(\varphi).\ ♣$$

Ex. 345

a) Si A es un anillo unitario, demostrar que existe un único homomorfismo de anillos Φ $\mathbf{Z} \to A$. Consecuentemente, tiene sentido la definición

$$carac(A) = n \quad \Leftrightarrow \quad Ker(\Phi) = (n).$$

b) Encontrar anillos de característica $0, 1, 2, \ldots$.

$\equiv$

a) Para cada $n \in \mathbf{Z}$, definimos

$$a_n := \begin{cases} 1+1+\overset{(n)}{\ldots}+1, & \text{si } n > 0, \\ 0, & \text{si } n = 0, \\ -1-1-\overset{(n)}{\ldots}-1, & \text{si } n < 0, \end{cases}$$

y fijamos

$$\begin{aligned} \Phi : \mathbf{Z} &\longrightarrow A \\ n &\to \Phi(n) := a_n. \end{aligned}$$

Es evidente que la aplicación Φ está bien definida. Veamos que es un homomorfismo de anillos: Sean $n, m \in \mathbf{Z}$

$$\begin{aligned} \Phi(n+m) &= a_{n+m} = a_n + a_m = \Phi(n) + \Phi(m) \\ \Phi(nm) &= a_{nm} = a_n a_m = \Phi(n)\Phi(m). \end{aligned}$$

Para ver que Φ es el único homomorfismo existente entre dichos anillos, sea $\varphi : \mathbf{Z} \to A$ un homomorfismo de anillos. Como todo homomorfismo de anillos transforma el cero de uno en el cero del otro, y lo mismo sucede con las unidades, tenemos que: $\varphi(0) = 0 = \Phi(0)$; $\varphi(1) = 1 = \Phi(1)$. Por tanto

$$\forall n \in \mathbf{Z}, n > 0, \quad \varphi(n) = \varphi(1+\overset{(n)}{\ldots}+1) = \varphi(1)+\overset{(n)}{\ldots}+\varphi(1) = 1+\overset{(n)}{\ldots}+1 = a_n = \Phi(n).$$

Si $n \in \mathbf{Z}$, $n < 0$, el razonamiento es similar. Así pues, $\varphi = \Phi$.

La definición dada arriba de la característica del anillo A tiene sentido ya que, como $Ker(\Phi)$ es un ideal de $\mathbf{Z}$ y éste es un anillo de ideales principales, se tiene que existe $n \in \mathbf{N}$, claramente único, tal que $Ker(\Phi) = (n)$. Además, la definición dada es coherente con el significado de característica, ya que, si para algún $n \in \mathbf{N}$ se tiene que $0 = n \cdot 1 = 1+\overset{(n)}{\ldots}+1 = \Phi(n)$, entonces $n \in Ker(\Phi)$.

b)

Caracteristica	Anillo	
0	$\mathbf{Z}$	
1	$\{0\}$,	ya que $Ker(\Phi) = (1) = \mathbf{Z}$
2	$\mathbf{Z}_2$,	ya que $Ker(\Phi) = (2) = 2\mathbf{Z}$
3	$\mathbf{Z}_3$,	ya que $Ker(\Phi) = (3) = 3\mathbf{Z}$
.....		
.....		
k	$\mathbf{Z}_k$,	ya que $Ker(\Phi) = (k) = k\mathbf{Z}$
.....		
.....		.

Para comprender mejor la aparición de estos ejemplos, consideremos uno de ellos, notar que, en general, el homomorfismo Φ es sobre, ya que $A = (\ 1\ )$ implica que, si $a \in A$, existe $n \in \mathbf{Z}$ tal que $a = a_n = \Phi(n)$.

$$carac(A) = 3 \leftrightarrow Ker(\Phi) = (\ 3\ ) \leftrightarrow A \cong \mathbf{Z}/Ker(\Phi) = \mathbf{Z}/(\ 3\ ) = Z_3. \clubsuit$$

Ex. 346 *Demostrar que la característica de un dominio de integridad es* $0, 1$ *ó un número primo.*

≡

Sea D un dominio de integridad de característica k. Suponiendo que $k \notin \{0, 1\}$ demostramos que k es primo. Sean $p, q \in \mathbf{N}$ tales que $k = pq$. Utilizando la notación del ejercicio previo, sabemos que $Ker(\Phi) = (\ k\ )$. Entonces

$$0 = \Phi(k) = \Phi(p)\Phi(q) \overset{(D\ dom.integ.)}{\rightarrow} \left\{ \begin{array}{cccc} \Phi(p) = 0 \rightarrow & p \in Ker(\Phi) \rightarrow & k \mid p \rightarrow & p = k \\ \acute{o} & \acute{o} & \acute{o} & \acute{o} \\ \Phi(q) = 0 \rightarrow & q \in Ker(\Phi) \rightarrow & k \mid q \rightarrow & q = k. \clubsuit \end{array} \right.$$

Ex. 347 *Si* $carac(A_1) = k_1$ *y* $carac(A_2) = k_2$, *hallar la característica del anillo producto* $A_1 \times A_2$.

≡

Primero veamos que, llamando $\Phi_1 : \mathbf{Z} \rightarrow A_1$, $\Phi_2 : \mathbf{Z} \rightarrow A_2$ a los homomorfismos tales que $Ker(\Phi_1) = (\ k_1\ )$ y $Ker(\Phi_2) = (\ k_2\ )$, respectivamente, entonces la aplicación $\Phi : \mathbf{Z} \rightarrow A_1 \times A_2$ tal que $\Phi(n) := (\Phi_1(n), \Phi_2(n))$ es un homomorfismo de anillos tal que $Ker(\Phi) = Ker(\Phi_1) \cap Ker(\Phi_2)$:

$$\begin{array}{l} \Phi(n+m) = (\Phi_1(n+m), \Phi_2(n+m)) = (\Phi_1(n) + \Phi_1(m), \Phi_2(n) + \Phi_2(m)) \\ = (\Phi_1(n), \Phi_2(n)) + (\Phi_1(m), \Phi_2(m)) = \Phi(n) + \Phi(m) \end{array}$$

$$\begin{array}{l} \Phi(nm) = (\Phi_1(nm), \Phi_2(nm)) = (\Phi_1(n)\Phi_1(m), \Phi_2(n)\Phi_2(m)) \\ = (\Phi_1(n), \Phi_2(n))(\Phi_1(m), \Phi_2(m)) = \Phi(n)\Phi(m). \end{array}$$

$$\begin{array}{l} n \in Ker(\Phi) \leftrightarrow (0,0) = \Phi(n) = (\Phi_1(n), \Phi_2(n)) \\ \leftrightarrow \left\{ \begin{array}{l} \Phi_1(n) = 0 \leftrightarrow n \in Ker(\Phi_1) \\ \Phi_2(n) = 0 \leftrightarrow n \in Ker(\Phi_2) \end{array} \right\} \Leftrightarrow n \in Ker(\Phi_1) \cap Ker(\Phi_2). \end{array}$$

Veamos finalmente que

$$carac(A_1 \times A_2) = \left\{ \begin{array}{ll} 0, & \text{si } k_1 = 0,\ \acute{o},\ k_2 = 0, \\ mcm(k_1, k_2), & \text{si } k_1 \neq 0,\ y,\ k_2 \neq 0. \end{array} \right.$$

Si, por ejemplo, $k_1 = 0$, entonces $Ker(\Phi_1) = (\ 0\ ) = \{0\}$ implica que $Ker(\Phi) = Ker(\Phi_1) \cap Ker(\Phi_2) = \{0\}$. Por tanto, $carac(A_1 \times A_2) = 0$. Supongamos que $k_1 \neq 0$ y $k_2 \neq 0$. Entonces sabemos que en $\mathbf{Z}$ siempre se cumple que la intersección de dos ideales es el ideal generado por el mínimo común múltiplo de los generadores. Así

$$Ker(\Phi) = Ker(\Phi_1) \cap Ker(\Phi_2) = (\ k_1\ ) \cap (\ k_2\ ) = (\ mcm(k_1, k_2)\ ).$$

Por tanto, $carac(A_1 \times A_2) = mcm(k_1, k_2)$. $\clubsuit$

Ex. 348 *Determinar el número de homomorfismos de anillos entre* $\mathbf{Z}_n$ *y* $\mathbf{Z}_m$.

$\equiv$

Sea $\varphi : \mathbf{Z}_n \to \mathbf{Z}_m$ un homomorfismo de anillos. Entonces, como $\varphi([0]_n) = [0]_m$ y $\varphi([1]_n) = [1]_m$, tenemos que, si $n < m$, entonces

$$[0]_m = \varphi([0]_n) = \varphi([n]_n) = \varphi([1]_n + \overset{(n)}{\cdots} + [1]_n) = [1]_m + \overset{(n)}{\cdots} + [1]_m = [n]_m \neq [0]_m,$$

lo que es absurdo. Por tanto, $n \geq m$. Dividiendo $n = mq + r$, $q, r \in \mathbf{Z}$, $0 \leq r < m$. Ahora

$$\begin{aligned}[0]_m = \varphi([0]_n) = \varphi([n]_n) = \varphi([qm + r]_n) &= \varphi([1]_n + \overset{(qm)}{\cdots} + [1]_n) + \varphi([1]_n + \overset{(r)}{\cdots} + [1]_n) \\ &= ([1]_m + \overset{(qm)}{\cdots} + [1]_m) + ([1]_m + \overset{(r)}{\cdots} + [1]_m) = [r]_m,\end{aligned}$$

de donde $r = 0$ y $n = qm$. Consecuentemente, se tiene lo siguiente actuación de φ

$\mathbf{Z}_n$		$\mathbf{Z}_m$
0	$\longrightarrow$	0
1	$\longrightarrow$	1
.....		
m	$\longrightarrow$	0
$m+1$	$\longrightarrow$	1
.....		
.....		
$(q-1)m$	$\longrightarrow$	0
$(q-1)m+1$	$\longrightarrow$	1
.....		
$qm-1$	$\longrightarrow$	$m-1$.

Así, una forma cómoda de expresar φ es: $\varphi([x]_n) = [x]_m$. Veamos que esta aplicación es en efecto homomorfismo de anillos.
φ bien definida: Si $[x]_n = [y]_m$, entonces $n \mid (x - y)$, lo que implica que $m \mid (x - y)$. Por lo tanto, $\varphi([x]_n) = [x]_m = [y]_m = \varphi([y]_n)$.
φ homomorfismo de anillos: Si $[x]_n, [y]_m \in \mathbf{Z}_n$, entonces

$$\varphi([x]_n + [y]_n) = \varphi([x + y]_n) = [x + y]_m = [x]_m + [y]_m = \varphi([x]_n) + \varphi([y]_n)$$

$$\varphi([x]_n[y]_n) = \varphi([xy]_n) = [xy]_m = [x]_m[y]_m = \varphi([x]_n)\varphi([y]_n).$$

Así pues, resumiendo

$$\text{N° de homomorfismos de anillos entre } \mathbf{Z}_n \text{ y } \mathbf{Z}_m = \begin{cases} 0, & \text{si } m \not| n, \\ 1, & \text{si } m \mid n. \end{cases} \clubsuit$$

Ex. 349 *Sea* φ *un epimorfismo entre los anillos* A *y* A'. *Si* I' *y* J' *son ideales de* A *y de* A', *respectivamente, demostrar*

a) $\varphi^{-1}(I' + J') = \varphi^{-1}(I') + \varphi^{-1}(J')$.

b) $\varphi^{-1}(I'J') = \varphi^{-1}(I')\varphi^{-1}(J')$.

$\equiv$

Recordemos que un epimorfismo es un homomorfismo suprayectivo.

a)

$[\subset]$

$$\forall z \in \varphi^{-1}(I'+J') \rightarrow \ \varphi(z) \in I'+J' \rightarrow \ \exists x' \in I', \exists y' \in J' \ / \ \varphi(z) = x'+y'.$$

Como φ es sobre, existen $x, y \in A$ tales que $\varphi(x) = x'$, $\varphi(y) = y'$. Así

$$\varphi(z) \ = \ x'+y' \ = \ \varphi(x)+\varphi(y) \ = \ \varphi(x+y) \ \rightarrow \ z-(x+y) \in Ker(\varphi),$$

lo que nos dice que $z = (x+y)+[z-(x+y)] \in \varphi^{-1}(I')+\varphi^{-1}(J')+Ker(\varphi) = \varphi^{-1}(I')+\varphi^{-1}(J')$, ya que $Ker(\varphi) \subset \varphi^{-1}(I') \cap \varphi^{-1}(J')$.

$[\supset]$ Se cumple en general, pues

$$I' \cup J' \ \subset \ I'+J' \ \rightarrow \ \varphi^{-1}(I')+\varphi^{-1}(J') \ \subset \ \varphi^{-1}(I'+J').$$

b)

$[\subset]$

$$\forall z \in \varphi^{-1}(I'J') \rightarrow \ \varphi(z) \in I'J'$$

$$\rightarrow \ \exists n \in \mathbf{N}, \exists x'_1, ..., x'_n \in I', \exists y'_1, ..., y'_n \in J' \ / \ \varphi(z) = x'_1y'_1 + ... + x'_ny'_n.$$

Como φ es sobre, para $i = 1, 2, ..., n$, existen $x_i, y_i \in A$ tales que $\varphi(x_i) = x'_i$, $\varphi(y_i) = y'_i$, $1 \leq i \leq n$. Así

$$\varphi(z) \ = \ \sum_{i=1}^{n} x'_iy'_i \ = \ \sum_{i=1}^{n} \varphi(x_i)\varphi(y_i) \ = \ \varphi(\sum_{i=1}^{n} x_iy_i) \ \rightarrow \ z - \sum_{i=1}^{n} x_iy_i \in Ker(\varphi),$$

ello nos dice que $z = \sum_{i=1}^{n} x_iy_i + (z - \sum_{i=1}^{n} x_iy_i) \in \varphi^{-1}(I')\varphi^{-1}(J') + Ker(\varphi) = \varphi^{-1}(I')\varphi^{-1}(J')$, ya que $Ker(\varphi) \subset \varphi^{-1}(I') \cap \varphi^{-1}(J') \subset \varphi^{-1}(I')\varphi^{-1}(J')$.

$[\supset]$ Sean $x \in \varphi^{-1}(I')$, $y \in \varphi^{-1}(J')$. Entonces

$$\varphi(xy) \ = \ \varphi(x)\varphi(y) \ \in \ I'J' \ \rightarrow \ xy \in \varphi^{-1}(I'J').$$

Ello implica, de la definición de producto de ideales, que $\varphi^{-1}(I')\varphi^{-1}(J') \subset \varphi^{-1}(I'J')$. ♣

Ex. 350 *Dados un anillo unitario conmutativo A y los ideales I, J tales que $I \subset J$, consideramos los anillos cociente A/I y A/J. Demostrar que la aplicación $\Phi : A/I \rightarrow A/J$ tal que $\Phi(x+I) = x+J$ es un epimorfismo de anillos y hallar su núcleo.*

$\equiv$

Φ bien definida: Sean $x, y \in A$ tales que $x+I = y+I$. Entonces, $x-y \in I \subset J$, nos dice que $x+J = y+J$, es decir, $\Phi(x+I) = \Phi(y+I)$.

Φ homomorfismo: Dados $x+I, y+I \in A/I$

$$\Phi[(x+I)+(y+I)] = \Phi[(x+y)+I] = (x+y)+J$$
$$= (x+J)+(y+J) = \Phi(x+I)+\Phi(y+I)$$

$$\Phi[(x+I)(y+I)] = \Phi[(xy)+I] = (xy)+J$$
$$= (x+J)(y+J) = \Phi(x+I)\Phi(y+I).$$

Φ sobre: Dado $y+J \in A/J$, buscamos $x+I \in A/I$ de modo que $\Phi(x+I) = y+J$. Basta tomar $x := y$.
Núcleo de Φ:

$x+I \in Ker(\Phi) \leftrightarrow J = \Phi(x+I) = x+J \leftrightarrow x \in J \Rightarrow Ker(\Phi) = J/I = \{x+I : x \in J\}$. ♣

Ex. 351 *Sea* $I = \{a+b\mathbf{i} \in \mathbf{Z}(\mathbf{i}) : a \equiv b \ (mod.\ 2)\}$. *Describir el anillo cociente* $\mathbf{Z}(\mathbf{i})/I$.

≡

Veamos primero que I es efectivamente un ideal de $\mathbf{Z}(\mathbf{i})$.

$$a+b\mathbf{i}, c+d\mathbf{i} \in I,\ x+y\mathbf{i} \in \mathbf{Z}(\mathbf{i}) \rightarrow$$

$$\begin{cases} a \equiv b \ (mod.\ 2),\ c \equiv d \ (mod.\ 2) \rightarrow (a-c) \equiv (b-d) \ (mod.\ 2) \\ \rightarrow (a+b\mathbf{i}) - (c+d\mathbf{i}) = (a-c) + /b-d)\mathbf{i} \in I. \\ b = a+2p \rightarrow (xa-yb) - (xb+ya) = x(a-b) - y(a+b) \\ = 2xp - 2y(a+p) \rightarrow (xa-yb) \equiv (ya+xb) \ (mod,2) \\ \rightarrow (x+y\mathbf{i})(a+b\mathbf{i}) = (xa-yb) + (xb+ya)\mathbf{i} \in I. \end{cases}$$

Finalmente, demostramos que el anillo cociente $\mathbf{Z}(\mathbf{i})/I$ es

$$\mathbf{Z}(\mathbf{i})/I = \{ I,\ 1+I \}.$$

Puesto que la inclusión recíproca es inmediata, veamos la inclusión directa. Si $a+b\mathbf{i} \in \mathbf{Z}(\mathbf{i})$, consideramos dos posibilidades
Una. $a \equiv b \ (mod.\ 2)$. Entonces, de la definición de I se tiene que $(a+b\mathbf{i})+I = I$.
Dos. $a \not\equiv b \ (mod.\ 2)$. Ahora tenemos que $a-b = 2p+1$, para cierto $p \in \mathbf{Z}$. Así

$$\left.\begin{array}{l} (a+b\mathbf{i}) - 1 = (a-1) + b\mathbf{i} \\ (a-1) - b = 2p \end{array}\right\} \rightarrow (a+b\mathbf{i}) - 1 \in I \rightarrow (a+b\mathbf{i}) + I = 1+I. \ \clubsuit$$

Nota 36 Conviene saber que en lo que se refiere a la descripción de estructuras cociente, A/I por ejemplo, el siguiente procedimiento " algorítmico"suele aplicarse frecuentemente:

1) Buscar otro anillo A' y un homomorfismo $\varphi : A \rightarrow A'$ tal que
2) $Ker(\varphi) = I$
3) φ sea sobre
4) Entonces, del teorema del isomorfismo de anillos, se tiene que $A/I \cong A'$.

Aplicando este algoritmo al ejercicio que acabamos de resolver

$$\begin{array}{rcl} \varphi & : & \mathbf{Z}(\mathbf{i}) \longrightarrow \mathbf{Z}_2 \\ & & a+b\mathbf{i} \ \rightarrow \ \varphi(a+b\mathbf{i}) := \overline{a-b}. \end{array}$$

Así

$$a+b\mathbf{i} \ \in \ Ker(\varphi) \ \leftrightarrow \ \overline{a-b} = \overline{0} \ \leftrightarrow \ a \equiv b \ (mod,2) \ \leftrightarrow \ a+b\mathbf{i} \ \in \ I.$$

Por tanto

$$\mathbf{Z}(\mathbf{i})/I \ \cong \ \mathbf{Z}_2 \ .$$

Ex. 352 *Sea $C[0,1]$ el anillo de las funciones reales continuas definidas en $[0,1]$. Consideremos el ideal $I = \{ \ f \in C[0,1] \ : \ f(\frac{1}{2}) = 0\}$. Describr el anillo cociente $C[0,1]/I$.*

≡

Es inmediato comprobar que I es un ideal de $C[0,1]$. Veamos que $C[0,1]/I$ es (isomorfo a) el anillo (cuerpo en realidad) de los números reales. Para ello, definimos

$$\begin{array}{rcl} \psi & : & C[0,1] \longrightarrow \mathbf{R} \\ & & f \ \rightarrow \ \psi(f) := \ f(\frac{1}{2}). \end{array}$$

ψ homomorfismo de anillos: Sean $f, g \in C[0,1]$

$$\begin{array}{l} \psi(f+g) = f(\frac{1}{2}) + g(\frac{1}{2}) = \psi(f) + \psi(g) \\ \psi(fg) = f(\frac{1}{2})g(\frac{1}{2}) = \psi(f)\psi(g). \end{array}$$

ψ sobre: Dado $\lambda \in \mathbf{R}$, consideremos la función constante $f : [0,1] \rightarrow \mathbf{R}$ tal que $f(x) = \lambda, \ x \in [0,1]$. Claramente, $f \in C[0,1]$ y $\psi(f) = f(\frac{1}{2}) = \lambda$.
$Ker(\psi) = I$:

$$f \in Ker(\psi) \ \leftrightarrow \ 0 = \psi(f) = f(\frac{1}{2}) \ \leftrightarrow \ f \in I.$$

Aplicando el teorema del isomorfismo para anillos, tenemos que

$$C[0,1]/I = C[0,1]/Ker(\psi) \ \cong \ \psi(C[0,1]) = \mathbf{R}. \ \clubsuit$$

Nota 37 El hecho de que el anillo cociente anterior nos haya salido isomorfo a un cuerpo no debe asustarnos. Ello es debido a que I es un ideal maximal de $C[0,1]$, como vemos a continuación: Si J es un ideal de $C[0,1]$ tal que $J \supset I$, entonces existe $f \in J$ tal que $f(\frac{1}{2}) \neq 0$. Consideremos la función $g(x) := x - \frac{1}{2}$. Claramente, $g \in I \subset J$. Ahora, la función $h(x) := f(x)^2 + g(x)^2$ pertenece a J. Pero h es un elemento unitario de $C[0,1]$, ya que $h(x) > 0, \ x \in [0,1]$. Consecuentemente, $\frac{1}{h(x)} \in C[0,1]$. Ello implica que $J = I$.

Capítulo 5

Apéndice: Integrales no elementales

5.1. Integrales que no salen

Cuando uno empieza a dar un primer curso de integración de funciones, el primer paso, después de recordar la no-tan-bien-apreciada afirmación "para ser un mediocre integrador es necesario ser un excelente derivador", introduce una lista de las llamadas *Integrales Inmediatas*. A partir de ahí se estudian una serie de métodos de càlculo de *primitivas*, o *antiderivadas*, o como a mí personalmente me gusta llamarlas, *integrales indefinidas*. Total, que el estudiante recibe una buena cantidad de información acerca de cómo calcular la integral de una función cualquiera; bueno, de cualquier función no. Como sabe todo profesor, y también todo estudioso de la materia, hay funciones bastante sencillas de escribir que no se pueden integrar, como por ejemplo las siguientes: $e^{\pm x^2}$, $\frac{e^x}{x}$, $\frac{1}{\log x}$, $\frac{\sin x}{x}$, $\frac{\cos x}{x}$, etc. El objetivo principal de este apéndice es simplemente explicar de manera divulgativa, pero bastante rigurosa, qué significa que una función no pueda ser integrada elementalmente.

Para clarificar la teoría que queremos explicar, necesitamos empezar definiendo de manera clara y concisa lo que se entiende por una *función elemental*, para después enunciar sin demostrar el *Teorema de Liouville* y algunas consecuencias que nos ayudarán a comprender porqué las funciones antes mencionadas no tienen integrales elementales. Como acabamos de indicar, fué el matemàtico francés Joseph Liouville, entre 1830 y 1840, quien hizo la aportación más importante dentro de esta problemàtica estableciendo que las integrales elementales, cuando existen, han de tener la siguiente forma: una función que pertenece al mismo *cuerpo diferencial* que la función del integrando más una cantidad finita de logaritmos de funciones de ese mismo cuerpo.

5.2. Funciones elementales

Recordemos primero que por un *cuerpo algebraico de funciones* entendemos un conjunto K formado por funciones de una parte de la recta real $\mathbf{R}$ en el conjunto de los números complejos $\mathbf{C}$ que cumple que, si $f, g \in K$, entonces $f - g$, $fg \in K$ i, si $f \neq 0$, también se tiene que $\frac{1}{f} \in K$. Si K es un cuerpo algebraico (siempre de funciones), dado un elemento $f \in K$, al escribir f' nos referimos a la función que se obtiene al hacer la derivada de f en los puntos de $\mathbf{R}$ donde dicha derivada exista. Un tal cuerpo K se dice que es un cuerpo diferencial siempre que cumple que: $\forall f \in K, \quad f' \in K$. Conviene observar que, si por $\mathbf{C}(x)$ representamos el cuerpo algebraico formado por todas las fracciones polinòmicas de coeficientes en $\mathbf{C}$, entonces $\mathbf{C}(x)$ és un cuerpo diferencial, es decir, como todos sabemos, la derivada de una fracción polinòmica es otra fracción polinòmica.

Definición 2 [Elemento algebraico]
Si tenemos un cuerpo diferencial K, una función φ, que puede no pertenecer a K, es un elemento algebraico sobre K siempre que existe un polinomio con coeficientes en K, $P \in K[x]$, $P \neq 0$, tal que $P(\varphi) = 0$. Evidentemente, todo elemento f de K es algebraico sobre K, simplemente tomemos el polinomio $P(x) := x - f \in K[x]$. Cuando una función no es algebraica sobre K se dice que es *trascendente* sobre K.

Definición 3 [Extensión algebraica]
Si tenemos dos cuerpos diferenciales K, E tales que $K \subseteq E$, E es una extensión algebraica de K siempre que existe $\varphi \in E$ tal que φ es algebraica sobre K y $E = K(\varphi)$, donde $K(\varphi)$ representa el menor cuerpo que contiene a K y a φ.

Definición 4 [Extensión logarítmica]
Si tenemos dos cuerpos diferenciales K, E tales que $K \subseteq E$, E es una extensión logarítmica de K siempre que existe $\varphi \in E$ tal que φ es trascendente sobre K, $E = K(\varphi)$, y se cumple que $\exists f \in K$ tal que $\varphi' = \frac{f'}{f}$ (notar que de alguna forma estamos diciendo que φ tiene que ver con $\log f$).

Definición 5 [Extensión exponencial]
Si tenemos dos cuerpos diferenciales K, E tales que $K \subseteq E$, E es una extensión exponencial de K siempre que existe $\varphi \in E$ tal que φ es trascendente sobre K, $E = K(\varphi)$, y se cumple que $\exists f \in K$ tal que $\varphi' = \varphi f'$ (notar que de alguna forma estamos diciendo que φ tiene que ver con e^f).

Definición 6 [Extensión elemental]
Si tenemos dos cuerpos diferenciales K, E tales que $K \subseteq E$, E es una extensión elemental de K siempre que existan $\varphi_1, \varphi_2, ..., \varphi_n \in E$ tales que $E = K(\varphi_1, \varphi_2, ..., \varphi_n)$, y se cumpla que $\forall j = 1, 2, ..., n$, $K(\varphi_1, \varphi_2, ..., \varphi_j)$ es una extensión, o bien algebraica, o bien logarítmica, o bien exponencial, de $K(\varphi_1, \varphi_2, ..., \varphi_{j-1})$.

Definición 7 [Función elemental]
Una función f, de una parte de $\mathbf{R}$ en $\mathbf{C}$, es una funció elemental siempre que existe alguna extensión elemental E de $\mathbf{C}(x)$ tal que $f \in E$.

A continuación visitamos algunos ejemplos de funciones elementales que nos indican que casi todas las funciones que manipulamos frecuentemente son elementales.

Ex. 353 La función $e^{g(x)}$, $g \in \mathbf{C}(x)$, g no constante, es elemental.

$\equiv$ Considerando el cuerpo $\mathbf{C}(x, e^{g(x)})$, tenemos que se trata de una extensión exponencial de $\mathbf{C}(x)$, ya que, tomando $f := g$, se tiene que $f \in \mathbf{C}(x)$, y, $(e^g)' = e^g \cdot f'$. ♣

Ex. 354 La función $\log x$ también es elemental.

$\equiv$ Tomando $f := x \in \mathbf{C}(x)$, está claro que $\mathbf{C}(x, \log x)$ es una extensión logarítmica de $\mathbf{C}(x)$ (por tanto una extensión elemental), ya que $(\log x)' = \frac{f'}{f}$. ♣

Los ejemplos que damos a continuación justifican el porqué estamos trabajando con funciones a valores complejos.

Ex. 355 Las funciones $\sin x$, $\cos x$ son elementales.

$\equiv$ Claramente, de la fòrmula de Euler: $e^{ix} = \cos x + i \cdot \sin x$, $x \in \mathbf{R}$, se deduce que

$$\begin{array}{l} \sin x = \frac{e^{ix}-e^{-ix}}{2i} \in \mathbf{C}(x, e^{ix}) \equiv \ Ext.exp.\ de\ \mathbf{C}(x) \\ \cos x = \frac{e^{ix}+e^{-ix}}{2} \in \mathbf{C}(x, e^{ix}) \equiv \ Ext.exp.\ de\ \mathbf{C}(x). \ \clubsuit \end{array}$$

Ex. 356 La función $\arctan x$ también es elemental.

$\equiv$ La demostración de esta afirmación requiere un poco más de conocimiento de las funciones complejas. Estudiemos la función $\log(\frac{x+i}{x-i})$ para ver que està relacionada con $\arctan x$. Antes, vamos a recordar la función logarítmica compleja: Si $w = \log z$, donde $w, z \in \mathbf{C}$, por definición se tiene que $e^w = z$. Si $w = x + yi$, entonces

$$z = e^w \Rightarrow z = e^{x+yi} = e^x(\cos y + i \cdot \sin y) \Rightarrow \left\{ \begin{array}{l} |z| = e^x \\ arg(z) = y \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} x = \log|z| \\ y = arg(z) \in]-\pi, \pi] \end{array} \right\}$$

$$\Rightarrow \log z = w = x + yi = \log|z| + i \cdot arg(z).$$

Aplicando la definición anterior del logaritmo (a la determinación escogida, ya que en general $arg(z) = y + 2k\pi$, $k \in \mathbf{Z}$, se le llama logaritmo principal), como $|x + i| = |x - i| = \sqrt{1 + x^2}$, $arg(x - i) = \arctan(\frac{-1}{x}) = -\arctan(\frac{1}{x}) = -arg(x + i)$, tenemos que

$$\log(\frac{x+i}{x-i}) = \log(x+i) - \log(x-i) = \log(|x+i|) + i \cdot arg(x+i) - [\log(|x-i|) + i \cdot arg(x-i)]$$

$$= 2i \cdot arg(x+i) = 2i \cdot \arctan(\frac{1}{x}) = 2i \cdot (\frac{\pi}{2} - \arctan x). \qquad (5.1)$$

Nota. Demostramos por razones de completitud que $\forall x > 0$, $\arctan x + \arctan(\frac{1}{x}) = \frac{\pi}{2}$:

Llamando $f(x) := \arctan x + \arctan(\frac{1}{x})$, aplicando càlculo elemental de una variable real,

$$f'(x) = \frac{1}{1+x^2} + \frac{\frac{-1}{x^2}}{1+(\frac{1}{x})^2} = \frac{1}{1+x^2} - \frac{1}{1+x^2} = 0 \Rightarrow \exists k \in \mathbf{R} \ / \ f(x) = k, \ \forall x > 0$$

$$\Rightarrow si \ \ x = 1: \ \ k = f(1) = \arctan 1 + \arctan(\frac{1}{1}) = \frac{\pi}{4} + \frac{\pi}{4} = \frac{\pi}{2}$$

$$\Rightarrow \arctan x + \arctan(\frac{1}{x}) = f(x) = k = \frac{\pi}{2}.$$

De (5.1)

$$\arctan x = \frac{\pi}{2} - \frac{1}{2i}\log(\frac{x+i}{x-i}).$$

Consecuentmente, queda claro que $\arctan x \in \mathbf{C}(x, \log(\frac{x+i}{x-i}))$, pero $\mathbf{C}(x, \log(\frac{x+i}{x-i}))$ es una extensión logarítmica de $\mathbf{C}(x)$, ya que, tomando $f := \frac{x+i}{x-i} \in \mathbf{C}(x)$, se tiene que

$$(\log(\frac{x+i}{x-i}))' = \frac{f'}{f}. \ \clubsuit$$

Ex. 357 Las funciones $\arcsin x$, $\arccos x$ también son elementales.

$\equiv$ Es fàcil ver que, para $x > 0$ (por ejemplo)

$$\left.\begin{array}{l} \arcsin x = \arctan(\frac{x}{\sqrt{1-x^2}}) \\ \arccos x = \arctan(\frac{\sqrt{1-x^2}}{x}) \end{array}\right\} \Rightarrow \arcsin x, \ \arccos x \in \mathbf{C}(x, \sqrt{1-x^2}, \log(\frac{\frac{x}{\sqrt{1-x^2}}+i}{\frac{x}{\sqrt{1-x^2}}-i})).$$

Claramente, $\mathbf{C}(x, \sqrt{1-x^2}, \log(\frac{\frac{x}{\sqrt{1-x^2}}+i}{\frac{x}{\sqrt{1-x^2}}-i}))$ es una extensión elemental de $\mathbf{C}(x)$, ya que:

$\sqrt{1-x^2}$ es un elemento algebraico sobre $\mathbf{C}(x)$ (simplemente consideremos $P(t) := (1-x^2) - t^2 \in \mathbf{C}(x)[t]$, y, $P(\sqrt{1-x^2}) = 0$), lo que implica que $\mathbf{C}(x, \sqrt{1-x^2})$ es una extensión algebraica de $\mathbf{C}(x)$.

Además, como hemos visto antes, $\mathbf{C}(x, \sqrt{1-x^2}, \log(\frac{\frac{x}{\sqrt{1-x^2}}+i}{\frac{x}{\sqrt{1-x^2}}-i})$ es una extensión logarítmica de $\mathbf{C}(x, \sqrt{1-x^2})$. $\clubsuit$

5.3. Teorema y Criterio de Liouville

Procedemos seguidamente a enunciar (sin demostrar, obviamente por su dificultad) el resultado fundamental de este apéndice.

Teorema 4 *[Teorema de Liouville]*

Sea f una función elemental y sea E una extensión elemental que contiene a f. Entonces: $\int f$ es una función elemental si y sólo si existen $\lambda_1, \lambda_2, ..., \lambda_n \in \mathbf{C}$, $g_1, g_2, ..., g_n \in E \setminus \{0\}$, y, $h \in E$, tales que

$$f = \lambda_1 \frac{g_1'}{g_1} + \lambda_1 \frac{g_2'}{g_2} + ... + \lambda_1 \frac{g_n'}{g_n} + h' .$$

Podemos reinterpretar el enunciado del teorema observando que entonces

$$\int f = \sum_{j=1}^{n} \lambda_j \log g_j + h .$$

Es decir, si f es elemental y está en E, la integral $\int f$ también está en E, excepto por una combinación lineal de logaritmos de funciones de E. A continuación, demostramos un resultado auxiliar que es fundamental en todo lo que sigue.

Lema 14 Sean $f_0, f_1, ..., f_n$ elementos de $\mathbf{C}(x)$. Sea $g \in \mathbf{C}(x)$, g no constante. Si

$$f_0(x) + f_1(x)e^{g(x)} + f_2(x)e^{2g(x)} + ... + f_n(x)e^{ng(x)} = 0,$$

entonces $f_0 = f_1 = ... = f_n = 0$. Es decir, $e^{g(x)}$ es trascendente sobre $\mathbf{C}(x)$.

$\equiv$ Hacemos la demostración por inducción sobre n. Para $n = 1$: Si tenemos que $f_0(x) + f_1(x)e^{g(x)} = 0$, con $f_0 = \frac{P_0}{Q_0}$, $f_1 = \frac{P_1}{Q_1}$, donde P_0, Q_0, P_1, Q_1 son polinomios, suponiendo que no se cumple nuestra tesis, podemos afirmar (multiplicando por $Q_0 \cdot Q_1$) que existen $R_0, R_1 \in \mathbf{C}[x]$ tales que $R_0 \neq 0$, $R_1 \neq 0$, $P_0 | R_0$, $P_1 | R_1$, y $R_0(x) + R_1(x)e^{g(x)} = 0$. Más aún, podemos suponer que R_0 y R_1 son primos entre sí (de no serlo, se divide por el màximo común divisor). Del Teorema Fundamental del Algebra, el polinomio R_0 admite alguna raíz compleja, sea $z \in \mathbf{C}$ tal que $R_0(z) = 0$. Por tanto, $R_1(z)e^{g(z)} = 0$. Pero, observemos que, si $g(z) = a + bi$,

$$0 = e^{g(z)} = e^{a+bi} = e^a \cdot e^{ib} = e^a(\cos b + i \cdot \sin b)$$

$$\Rightarrow \cos b + i \cdot \sin b = 0 \Rightarrow \left\{ \begin{array}{l} \cos b = 0 \\ \sin b = 0 \end{array} \right\} \Rightarrow \textit{Absurdo.}$$

Consecuentemente, como $e^{g(z)} \neq 0$, se tiene que $R_1(z) = 0$, lo que es una contradicción, ya que R_0 y R_1 no pueden tener raíces comunes.

Suponiendo ahora que la afirmación del enunciado vale para n, demostrémosla para $n + 1$: Partimos de que

$$f_0(x) + f_1(x)e^{g(x)} + f_2(x)e^{2g(x)} + ... + f_{n+1}(x)e^{(n+1)g(x)} = 0.$$

Entonces

$$e^{g(x)}[f_1(x) + f_2(x)e^{g(x)} + +... + f_{n+1}(x)e^{ng(x)}] = -f_0(x).$$

Si $f_0 = \frac{P_0}{Q_0}$, multiplicando por Q_0 obtenemos

$$e^{g(x)}[h_1(x) + h_2(x)e^{g(x)} + +... + h_{n+1}(x)e^{ng(x)}] = -P_0(x),$$

donde $h_j = Q_0 \cdot f_j \in \mathbf{C}(x)$, $1 \leq j \leq n+1$. Si el grado de P_0 es m, derivando $m+1$ veces obtenemos, aplicando la fòrmula de Leibnitz de las derivadas sucesivas de un producto,

$$0 = \sum_{k=0}^{m+1} \binom{m+1}{k} (e^{g(x)})^{(m+1-k)} \sum_{j=1}^{n+1} [h_j(x)e^{(j-1)g(x)}]^{(k)}.$$

Para cada $k = 0, 1, ..., m+1$, se puede ver fàcilmente que $(e^{g(x)})^{(m+1-k)} = r_k(x)e^{g(x)}$, con $r_k \in \mathbf{C}(x)$: Por tanto, permutando los sumatorios y dividiendo por $e^{g(x)}$

$$0 = \sum_{j=1}^{n+1} \sum_{k=0}^{m+1} \binom{m+1}{k} r_k(x)[h_j(x)e^{(j-1)g(x)}]^{(k)}.$$

Aplicando la hipòtesis de inducción, podemos afirmar que, para $j = 1, 2, ..., n+1$,

$$\sum_{k=0}^{m+1} \binom{m+1}{k} r_k(x)[h_j(x)e^{(j-1)g(x)}]^{(k)} = 0.$$

Multiplicando por $e^{g(x)}$, recordando la definición de las fracciones r_k, tenemos

$$\sum_{k=0}^{m+1} \binom{m+1}{k} (e^{g(x)})^{(m+1-k)}[h_j(x)e^{(j-1)g(x)}]^{(k)} = 0.$$

Pero, el primer miembro de la igualdad anterior es

$$[e^{g(x)}h_j(x)e^{(j-1)g(x)}]^{(m+1)} = [h_j(x)e^{jg(x)}]^{(m+1)} = 0.$$

Ello implica que $h_j(x)e^{jg(x)}$ es un polinomio, lo que no puede ser, ya que $j \neq 0$, (como se puede ver razonando anàlogamente a lo que hemos hecho para $n = 1$) a menos que $h_j = 0$. Por tanto, de la definición de h_j, $1 \leq j \leq n+1$, tenemos $f_1 = ... = f_{n+1} = 0$, y también $f_0 = 0$. ♣

Corolario 2 [Criterio de Liouville]

Si $f, g \in \mathbf{C}(x)$ son tales que $f \neq 0$, y, g no es constante, entonces:
$\int f(x)e^{g(x)}$ es elemental si y sólo si

$$\exists h \in \mathbf{C}(x) \ / \quad h' + g' \cdot h = f \ .$$

$\equiv$
($\Leftarrow$) Si $h'(x)+g'(x)h(x) = f(x)$, con $h \in \mathbf{C}(x)$, está claro que

$$f(x)\mathrm{e}^{g(x)} = (h'(x)+g'(x)h(x))\mathrm{e}^{g(x)} = [h(x)\mathrm{e}^{g(x)}]' \Rightarrow \int f(x)\mathrm{e}^{g(x)} = h(x)\mathrm{e}^{g(x)}+\lambda\ (\lambda \in \mathbf{C})$$

$$\Rightarrow \int f(x)\mathrm{e}^{g(x)} \in \mathbf{C}(x, \mathrm{e}^{g(x)}) \equiv \textit{Ext.exp. de } \mathbf{C}(x).$$

($\Rightarrow$) Supongamos que $\int f(x)\mathrm{e}^{g(x)}$ es elemental. Del Teorema de Liouville, considerando $\mathbf{C}(x, \mathrm{e}^{g(x)})$, que es extensión elemental de $\mathbf{C}(x)$, y que contiene $f(x)\mathrm{e}^{g(x)}$, sabemos que

$$f(x)\mathrm{e}^{g(x)} = \sum_{j=1}^{n} \lambda_j \frac{\varphi_j'(x)}{\varphi_j(x)} + \psi'(x), \quad \varphi_j \in \mathbf{C}(x, \mathrm{e}^{g(x)}) \setminus \{0\},\ 1 \leq j \leq n, \quad \psi \in \mathbf{C}(x, \mathrm{e}^{g(x)}). \tag{5.2}$$

Si indicamos por ∂ el grado de un elemento de $\mathbf{C}(x, \mathrm{e}^{g(x)})$ en $\mathrm{e}^{g(x)}$, observando que, por ejemplo la función $\varphi(x) = \sum_{k=0}^{m} P_k(x)\mathrm{e}^{kg(x)}$ tiene por derivada $\varphi'(x) = \sum_{k=0}^{m}(P_k'(x) + kg'(x)P_k(x))\mathrm{e}^{kg(x)}$, tenemos que $\partial(\frac{\varphi'}{\varphi}) = 0$. Por tanto, de (2), tomando grados

$$1 = \partial(f(x)\mathrm{e}^{g(x)}) = max\{\ 0,\ \partial(\psi')\}.$$

De donde, $\partial(\psi') = 1$ y, suponiendo que $\psi(x) = h(x)\mathrm{e}^{g(x)}$, se obtiene que $\psi'(x) = (h'(x) + g'(x)h(x))\mathrm{e}^{g(x)}$ y, de (2) otra vez

$$[f(x) - h'(x) - g'(x)h(x)]\mathrm{e}^{g(x)} - \sum_{j=1}^{n} \lambda_j \frac{\varphi_j'(x)}{\varphi_j(x)} = 0.$$

Como hemos visto antes que $\mathrm{e}^{g(x)}$ es trascendente sobre $\mathbf{C}(x)$, podemos afirmar que

$$f(x) = h'(x) + g'(x)h(x)\ . \clubsuit$$

Ex. 358 Las integrales $\int \mathrm{e}^{\pm x^2}$ no son elementales.

$\equiv$ Aplicando el Criterio de Liouville, si $\int \mathrm{e}^{\pm x^2}$ fuese elemental, existiría una función $h \in \mathbf{C}(x)$ tal que, tomando $f := 1$, $g(x) := x^2$ (se hace anàlogamente para e^{-x^2}), $h'(x) + h(x)(2x) = 1$. Ahora bien, como $h \in \mathbf{C}(x)$, existen dos polinomios $P, Q \in \mathbf{C}[x]$, $P \neq 0$, tales que $h(x) = \frac{P(x)}{Q(x)}$. Podemos asumir que los polinomios P, Q son primos entre sí. Entonces

$$1 = \frac{P'(x)Q(x) - P(x)Q'(x)}{Q(x)^2} + 2x\frac{P(x)}{Q(x)}.$$

Multiplicando por $Q(x)^2$

$$Q(x)^2 = P'(x)Q(x) - P(x)Q'(x) + 2xP(x)Q(x) = [P'(x)+2xP(x)]Q(x) - P(x)Q'(x),$$

de donde

$$P(x)Q'(x) = Q(x)[P'(x) + 2xP(x) - Q(x)]. \tag{5.3}$$

Distinguimos dos posibilidades que, como veremos, son absurdas, lo que demuestra que la integral no puede ser elemental:
Una. Q es constante. Entonces $0 = P'(x) + 2xP(x) - Q(x)$, pero $Q(x) = P'(x) + 2xP(x)$ implica que $0 = grau(Q) = grau(P'(x) + 2xP(x))$, absurdo, ya que, como $P \neq 0$, $grau(P'(x) + 2xP(x)) \geq 1$.
Dos. Q no es constante. En este caso, Q tiene alguna raíz compleja, es decir, $Q(z) = 0$, $z \in \mathbf{C}$. Suponiendo que la raíz z tiene multiplicidad m, podemos factorizar $Q(x) = (x-z)^m R(x)$, con $R(z) \neq 0$. De (3), $(x-z)^m$ es un divisor de $P(x)Q'(x) = P(x) \cdot (x-z)^{m-1}[mR(x) + (x-z)R'(x)]$. Ello implica que $x - z$ tiene que dividir $P(x)$, lo que contradice el hecho de que P, Q no tienen divisores comunes. ♣

Ex. 359 La integral $\int \frac{e^{\lambda x}}{x}$, $\lambda \neq 0$, no es elemental.

≡ Aplicando el Criterio de Liouville, si $\int \frac{e^{\lambda x}}{x}$ fuese elemental, existiría una función $h \in \mathbf{C}(x)$ tal que, tomando $f(x) := \frac{1}{x}$, $g(x) := \lambda x$, se cumple

$$\frac{1}{x} = h'(x) + h(x) \cdot \lambda.$$

Ahora bien, como $h \in \mathbf{C}(x)$, existen dos polinomios $P, Q \in \mathbf{C}[x]$, $P \neq 0$, tales que $h(x) = \frac{P(x)}{Q(x)}$. Podemos asumir que los polinomios P, Q son primos entre sí. Entonces

$$\frac{1}{x} = \frac{P'(x)Q(x) - P(x)Q'(x)}{Q(x)^2} + \lambda \frac{P(x)}{Q(x)}.$$

Multiplicando por $xQ(x)^2$

$$Q(x)^2 = x[P'(x)Q(x) - P(x)Q'(x)] + \lambda x P(x)Q(x);$$

$$Q(x)[Q(x) - xP'(x) - \lambda x P(x)] = -xP(x)Q'(x). \tag{5.4}$$

Como hemos hecho en el ejemplo anterior, distinguimos dos posibilidades que, como veremos, son absurdas, lo que demuestra que la integral no puede ser elemental:
Una. Q es constant. Entonces $Q(x) = x[P'(x) + \lambda P(x)]$, de donde tenemos un absurdo, ya que Q tiene grado cero y el polinomio $x[P'(x) + \lambda P(x)]$, como $P \neq 0$, no es constante.
Dos. Q no es constant. En este caso, Q tiene alguna raíz compleja, es decir, $Q(z) = 0$, $z \in \mathbf{C}$. Suponiendo que la raíz z tiene multiplicidad m, podemos factorizar $Q(x) = (x-z)^m R(x)$, con $R(z) \neq 0$. De (5.4), $(x-z)^m$ es un divisor de $xP(x)Q'(x)$, lo que implica que $x - z$ es divisor de $xP(x)$. Como z no puede ser raíz de P, tenemos que $x - z$ es divisor de x, es decir, $x - z = x$, y, $z = 0$. Entonces, tennemos que $Q(x) = x^m R(x)$, con $R(0) \neq 0$. Derivando $Q'(x) = mx^{m-1}R(x) + x^m R'(x)$, de donde tenemos que

$$x^m R(x) \mid xP(x)[mx^{m-1}R(x) + x^m R'(x)] = x^m P(x)[mR(x) + xR'(x)]$$

$$\Rightarrow R(x) \mid P(x)[mR(x) + xR'(x)].$$

Pero, como P, R son primos entre sí,

$$R(x) \mid mR(x) + xR'(x) \Rightarrow R(x) \mid xR'(x).$$

Al tener R y xR' el mismo grado, de la divisibilidad anterior, podemos asegurar la existencia de $a \in \mathbf{C}$ tal que $R(x) = a \cdot xR'(x)$. Eso nos lleva a que $R(0) = 0$, absurdo. ♣

Ex. 360 Las integrales $\int \frac{\sin x}{x}$, $\int \frac{\cos x}{x}$ no son elementales.

≡ Demostramos que $\int \frac{\sin x}{x}$ no es elemental, de manera anàloga se ve que $\int \frac{\cos x}{x}$ tampoco es elemental. Si $\int \frac{\sin x}{x}$ fuese elemental, como $\sin x = \frac{e^{ix}-e^{-ix}}{2i}$, tendríamos que la integral $\int \frac{e^{ix}-e^{-ix}}{x}$ también sería elemental. Aplicando el Teorema de Liouville, existen $\varphi_j \in \mathbf{C}(x, e^{ix})$, $c_j \in \mathbf{C}$, $1 \leq j \leq n$, $\psi \in \mathbf{C}(x, e^{ix})$ tales que

$$\frac{e^{ix} - e^{-ix}}{x} = \psi'(x) + \sum_{j=1}^{n} c_j \frac{\varphi_j'(x)}{\varphi_j(x)}.$$

Multiplicando por e^{ix}

$$\frac{e^{2ix} - 1}{x} = e^{ix} \cdot [\psi'(x) + \sum_{j=1}^{n} c_j \frac{\varphi_j'(x)}{\varphi_j(x)}].$$

De donde, tomando grados en e^{ix}

$$2 = max\{\partial(\psi'), 0\} + 1 \Rightarrow \partial(\psi') = 1.$$

Si $\psi'(x) = h(x)e^{ix} + r(x)$, $h, r \in \mathbf{C}(x)$, entonces

$$(\frac{1}{x} - h(x))e^{2ix} - (r(x) + \sum_{j=1}^{n} c_j \frac{\varphi_j'(x)}{\varphi(x)})e^{ix} - \frac{1}{x} = 0,$$

lo que es absurdo. ♣

Nota 38 Para terminar definitivamente, simplemente observar que el que la integral de una función no sea elemental implica que no importa el método de integración, o sea, cálculo de primitivas, que se emplee (aunque esté recién inventado y no se haya estudiado aún..., i.e., aviso para jóvenes ilusos...) el resultado no va a ser expresable como una función de las elementales, es decir, éso es lo que significamos al decir vulgarmente la integral de una función no sale.

Bibliografía

[1] G. BHIRKOFF, S. MCLANE, Algebra Moderna, *Ed. McGraw-Hill*, Madrid 1972.

[2] A. CLARK, Elementos de Algebra Abstracta, *Ed. Alahambra*, Madrid 1980.

[3] P. DUBREIL, Teoría de Grupos, *Ed. Reverté*, Barcelona 1970.

[4] J. A. GALLIAN, Contemporary Abstract Algebra, *D. C. Heath and Co.*, Lexington, Massachussets, 1986.

[5] C. R. HADLOCK, Field Theory and its classical problems, *Carus Math. Monographs*, Math. Assoc. of America, 1978.

[6] S. LANG, Algebra Moderna, *Ed. Reverté*, Barcelona 1977.